PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04H 1/00

A1

(11) International Publication Number: WO 99/21307

(43) International Publication Date: 29 April 1999 (29.04.99)

(21) International Application Number: PCT/US98/14070

(22) International Filing Date: 7 July 1998 (07.07.98)

(30) Priority Data:
08/954,455 20 October 1997 (20.10.97) US

(71) Applicant: MOTOROLA INC. [US/US]; 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

(72) Inventors: CUDAK, Mark, Conrad; 3318 Chestnut Drive, McHenry, IL 60050 (US). PEARCE, Michael, David; 1223 Berkshire Lane, Barrington, IL 60010 (US).

(74) Agents: STOCKLEY, Darleen, J. et al.; Motorola Inc., Intellectual Property Dept., 1303 East Algonquin Road, Schaumburg, IL 60196 (US).

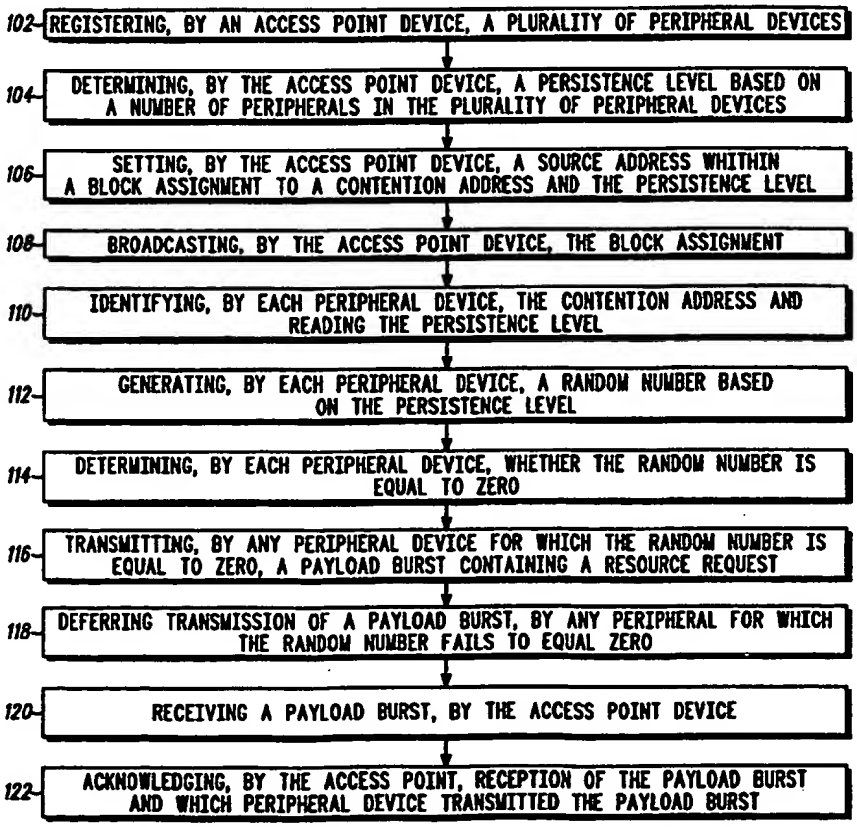
(81) Designated States: CN, DE, GB.

Published
With international search report.

(54) Title: LOW COMPLEXITY DYNAMIC PERSISTENCE MODE FOR RANDOM ACCESS IN A WIRELESS COMMUNICATION SYSTEM

(57) Abstract

A method, access point device and peripheral device provide low complexity dynamic persistence for random access in a wireless communication system (100). The peripheral device includes a block assignment receiver for receiving a block assignment having a source address which contains a contention address and a persistence level and for identifying the contention address and reading the persistence level; a random number generator coupled to the block assignment receiver for generating a random number based on the persistence level; and a persistence based transmitter coupled to the random number generator for transmitting a payload burst containing a resource request based on the random number and the persistence level.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

LOW COMPLEXITY DYNAMIC PERSISTENCE MODE FOR RANDOM ACCESS IN A WIRELESS COMMUNICATION SYSTEM

Related Applications

The present application is related to the following applications which are incorporated herein by reference: CR00180M, NETWORK PROTOCOL METHOD, ACCESS POINT DEVICE AND PERIPHERAL DEVICES FOR PROVIDING FOR AN EFFICIENT CENTRALLY COORDINATED PIER-TO-PIER WIRELESS COMMUNICATIONS NETWORK, by Mark Cudak, Bruce Mueller, James Kelton, and Brian Keith Classon, which is being filed concurrently on October 20, 1997, and which is assigned to Motorola, Inc. and CR00181M, METHOD, ACCESS POINT DEVICE AND PERIPHERAL FOR PROVIDING SPACE DIVERSITY IN A TIME DIVISION DUPLEX WIRELESS SYSTEM, by Bruce Eastmond, Mark Cudak and James Kepler, which is being filed concurrently on October 20, 1997, and which is assigned to Motorola, Inc.

Field of the Invention

The present invention relates to wireless communication systems, and more particularly, to centrally coordinated pier-to-pier wireless communication systems.

Background of the Invention

In a wireless communication system comprising of multiple devices sharing a common RF channel to transmit data, a medium access protocol governs the which peripheral has access to the RF channel at a specific moment of time and for a specified duration. Many medium access protocols are distributed where each peripheral operates as a pier performing identical algorithms to access the channel. In other protocols, one device may act as the master receiving requests for the channel access and granting service. In all these, systems their is opportunity for the RF transmissions from two peripheral devices to occur simultaneously, colliding and destructively interfering such that no information may be communicated. The medium access protocol must reduce the probability of collision to maximize the data transfer rate of the system as whole.

The amount of data each peripheral device has to transfer varies with time. Peripherals are generally bi-modal and exist in active or standby mode. Peripheral devices are active when they have data to send and inactive when no data is awaiting transmission. When active, the peripheral device accesses the channel transmits the data and returns to a standby mode. The probability of collision is a function of the number of peripherals in the system and the arrival rate of data to send.

A simple method for reducing the collisions is by not having each peripheral transmit with absolute certainty in the active mode. Rather, each peripheral will transmit with a

fixed probability. This probability is known as a persistence level. It has been shown, that persistence level can significantly reduce the probability of collision when the number of devices and their respective arrival rates are known. However, a fixed persistence level appropriate for a given number of devices may become sub-optimal if the number of devices or arrival rates change.

Most systems also employ a busy-tone or carrier sensing to improve the data transfer rate by insuring that once one peripheral device has seized the channel, no other peripheral device will begin transmitting. This method reduces the probability of collision by shortening the period that peripheral devices may contend for access to the system. Once peripheral device has seized the channel all other devices will defer transmission until that peripheral completes. During that transmission, many peripherals will transition from the standby to active mode and be ready to transmit data. The probability of collision immediately following a transmission is greatly increased. Collisions following the transmission compound the problem allowing a larger number of peripherals to transition to the active mode starting a catastrophic spiral where the newly active peripherals further contribute to the collisions such that no data is successfully transmitted.

In a multipurpose communication system, the channel may be shared by other types of transmissions which cause the channel to appear busy and the phenomenon described may occur whenever the channel transitions from busy to ideal.

A random back-off algorithm is nearly always employed to avoid the catastrophic cycle following the busy period. In a random back-off algorithm each peripheral device detects if the channel is busy or if there has been a collision and the waits a random period, called a back-off period, before attempting transmission. Subsequent collisions may require that the peripheral back-off for longer period which each successive collision. This type of algorithm is effective, however, it is complex. It requires that each contending peripheral maintain has a memory of the previous collisions requiring a complex state machine.

Thus there is a need for a method, an access point device and a peripheral device for providing low complexity dynamic persistence for random access by a peripheral device in a wireless communication system.

Brief Description of the Drawings

FIG. 1 is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention.

FIG. 2 is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random

access by a peripheral device in a wireless communication system in accordance with the present invention.

FIG. 3 is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random access by an access point device in a wireless communication system in accordance with the present invention.

FIG. 4 is a block diagram of a peripheral device for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention.

FIG. 5 is a block diagram of an access point device for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention.

FIG. 6 is a block diagram of one embodiment of a persistence based transmitter in accordance with the present invention.

FIGs. 7-27 provide illustrations in accordance with a preferred embodiment of the present invention.

Detailed Description of a Preferred Embodiment

The present invention provides a minimized complexity solution to low complexity dynamic persistence for random access of peripheral devices in a wireless communication system. Presently, peripheral devices typically retain a memory of prior events via state machines to keep track of contention attempts, and thus enter into further contention attempts in a predetermined timely manner. However, in the present invention, peripheral devices are memoryless, i.e., are not required to retain a memory of prior events. Thus, peripheral devices in the present invention are less complex.

Since the persistence mode is dynamic, a complex random back-off algorithm is not required. The back-log caused during a busy period is modeled as a change in the arrival rate and the persistence mode is adjusted accordingly. Furthermore, a dynamic persistence mode is more effective if the number of participating device is known to change. A central controlling device, called an access point device, aware of the number of devices and duration of the busy period systematically varies the persistence level, allowing for low-complexity peripheral devices.

FIG. 1, numeral 100, is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention. The method

includes the steps of: A) registering (102), by an access point device, a plurality of peripheral devices; B) determining (104), by the access point device, a persistence level based on a number of peripherals in the plurality of peripheral devices; C) setting (106), by the access point device, a source address within a block assignment to a contention address and the persistence level; D) broadcasting (108), by the access point device, the block assignment; E) identifying (110), by each peripheral device, the contention address and reading the persistence level; F) generating (112), by each peripheral device, a random number based on the persistence level; G) determining (114), by each peripheral device, whether the random number is equal to zero; H) transmitting (116), by any peripheral device for which the random number is equal to zero, a payload burst containing a resource request; I) deferring (118) transmission of a payload burst, by any peripheral for which the random number fails to equal zero; J) receiving (120) a payload burst, by the access point device; and K) acknowledging (122), by the access point, reception of the payload burst and which peripheral device transmitted the payload burst.

FIG. 2, numeral 200, is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random access by a peripheral device in a wireless communication system in accordance with the present invention. The method includes the steps of: A)

receiving (202) a block assignment having a source address which contains a contention address and a persistence level; B) identifying (204) the contention address and reading the persistence level; C) generating (206) a random number based on the persistence level; D) determining (208) whether the random number is equal to zero; and E) transmitting (210) when the random number is equal to zero and deferring transmission when the random number fails to equal zero.

FIG. 3, numeral 300, is a flow chart showing one embodiment of steps for providing low complexity dynamic persistence for random access by an access point device in a wireless communication system in accordance with the present invention. The method includes the steps of: A) registering (302) a plurality of peripheral devices; B) determining (304) a persistence level based on a number of peripheral devices in the plurality of peripheral devices; C) setting (306) a source address within a block assignment to a contention address and the persistence level; D) broadcasting (308) the block assignment; E) determining (310) whether a payload burst has been received; and F) acknowledging (312), where a payload burst has been received, reception of the payload burst and which peripheral device transmitted the payload burst.

Acknowledging may be selected to utilize assigning a number of blocks based on the resource request sent by the

peripheral transmitting the payload burst, or alternatively, to utilize assigning a destination address in a next block assignment which contains a source address equal to the contention address.

FIG. 4, numeral 400, is a block diagram of a peripheral device for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention. The peripheral device typically includes a block assignment receiver (402), a random number generator (404), and a persistence based transmitter (406). The block assignment receiver (402) receives a block assignment having a source address which contains a contention address and a persistence level and identifying the contention address and reading the persistence level. The random number generator (404), which is coupled to the persistence based transmitter (406) and is used for generating a random number based on the persistence level. The persistence based transmitter (406) is coupled to the random number generator (404) and to the block assignment receiver (402) and is used for transmitting a payload burst containing a resource request based on the random number and the persistence level.

In the preferred embodiment, the random number generator (404) is a linear feedback shift register generating a pseudorandom binary sequence wherein a number of bits

generated by the linear feedback shift register is based on the persistence level and the persistence based transmitter transmits the payload burst when the bits generated are all equal to zero.

Peripheral devices may typically be implemented in wireless speakers, cordless telephones, shared printers, networked games, peripheral personal computers (PCs), children's toys, video electrical devices, audio electrical devices, set top boxes and the like.

FIG. 5, numeral 500, is a block diagram of an access point device for providing low complexity dynamic persistence for random access in a wireless communication system in accordance with the present invention. The access point device generally includes a device manager (502), an efficient persistence scheduler (504), a transmitter (506), and a receiver (508). The device manager (502) is arranged to receive registration requests from a plurality of peripheral devices and registers the plurality of peripheral devices. In addition, the device manager (502) determines a persistence level based on a number of peripheral devices in the plurality of peripheral devices. The efficient persistence scheduler (504) is coupled to the device manager and the receiver (508) and is used for setting a source address within a block assignment to a contention address and the persistence level.

The transmitter (506) is coupled to the efficient persistence scheduler (504) and broadcasts the block assignment. The receiver (508) is coupled to the efficient persistence scheduler (504) and is arranged to receive a payload burst. The receiver (508) determines whether the payload burst containing a resource request has been received. Where a payload burst has been received, the receiver passes the resource request to the efficient persistence scheduler (504), which acknowledges reception of the resource request and which peripheral device transmitted the payload burst in a subsequent block assignment.

FIG. 6, numeral 600, is a block diagram of one embodiment of a persistence based transmitter in accordance with the present invention. The down counter (602) receives a persistence value from the block assignment receiver (402) when the reset signal is asserted (load) and also receives a clock value. A first OR gate (604) receives the output of the down counter (602) and in combination with the AND gate (606) gates the clock to a random number generator (linear feedback shift register, LFSR; 608) and an inverted version (610) of the clock to a one-bit latch (612). An second OR gate (614) is coupled to the LFSR (608) and to the one-bit latch (612) and combines a most recent value stored in the one-bit latch (612) and the output of the LFSR (608). The one-bit latch (612) receives a one-bit value from the OR gate (614) on a rising edge of the inverted version (610) of the clock and also

receives the reset signal (clear). An inverter (616) is coupled to the first OR gate (604) to provide a ready signal when the down counter (602) is all zeros. The output of the one-bit latch (612) is a TX-inhibit signal that is valid when the ready signal is asserted.

FIGs. 7-27 provide illustrations in accordance with a preferred embodiment of the present invention. A preferred embodiment of the present invention is described below: The 2.4 GHz Industrial, Scientific, and Medical (ISM) band is the only frequency band available on a worldwide basis for unlicensed devices, which makes it the ideal choice for consumer in-home networks.. In the U.S. it is governed by FCC parts 15.209 and 15.247. In Europe, ETSI ETS 300.328 outlines its requirements.. In Japan, RDR STD 33 covers the band. Throughout the rest of the world the ITU has designated this band for common use. The dominant application of this frequency band is for consumer microwave ovens which on one-hand guarantees the continued existence of the band but on the other hand is a significant source of interference. In spite of this challenge, this band provides an opportunity for in-home networks to be developed on one platform for universal deployment, allowing the greatest economy of scale to be leveraged.

Micro-cellular protocols such as DECT and PHS have been suggested for in-home applications and, at first glance, seem suitable with respect to their integral cordless telephone

function. However, in addition to the frequency band translations problems involved in moving DECT or PHS to a different band, the DECT and PHS protocols themselves are not conducive to operation in the 2.4 GHz ISM band. Both PHS and DECT cannot withstand the microwave interference guaranteed to be found in the home environment. Interference aside, these micro-cellular systems contain significant additional complexity to handle community or campus deployment providing for intercell hand-off and roaming capability. Similarly, they are designed to tolerate multi-path distortion present even in their small micro-cell environment significantly larger than an in-home pico-cell. A system designed solely for the in-home single pico-cell environment will be significantly less complex, and can be engineered to provide nearly transparent service in the presence of microwave interference.

The Dynamic Acknowledged Time Division Multiple Access (DA-TDMA) system proposed herein has been designed specifically for in-home networks with a consumer-market based low-cost design philosophy. The system design trades spectral efficiency for a strong signal-to-noise ratio over its pico-cell coverage area, allowing for near error-free transmission in the absence of interference. A low-complexity ARQ has been designed to handle periodic interference from microwave ovens co-resident in the ISM band. The physical layer and data link protocols are realizable in a custom silicon and would only require an 8-bit-class microprocessor for

configuration and initialization. The system is capable of providing data-rates as high as 1 Mbps (512 Kbps in severe microwave interference) for high performance data applications such as wireless-print sharing while supporting low-cost low-complexity automated appliance applications.

The value of wireless communications is becoming increasingly valuable to consumers. The growth of cellular and cordless telephony, combined with the promise of future high speed wireless data networks, is creating a market for wireless information devices in the home. The growth of computational power in consumer devices has enabled a number of services. Personal computers can now easily manage all of our communications, including electronic mail, voice messaging, call routing and prioritization. Computers are ideal for maintaining the many methods of communication to others, including phone numbers, fax numbers, email addresses, and postal addresses. However, their use for these purposes is inherently limited because the computer is typically located in a remote part of the consumer's dwelling. Set top boxes also hold the capability to provide central communications services in the consumer's living room. However, their utility is also limited because typically their associated television display is located far away from a telephone jack.

This DA-TDMA specification enables the PC and the set-top box to extend their reach into the entire consumer household. A variety of familiar and new devices are enabled,

such as advanced cordless phones, handheld browsers, smart children's toys, and cordless printing. Access to data on the home computer as well to the Internet can be seamlessly delivered to devices, while several simultaneous voice conversations are in progress. By utilizing speech recognition/synthesis on a remote computer, voice enabled portable devices may become common. The inherent low complexity of this standard combined with the operation in a worldwide ISM band will allow a significant market volume to drive the devices to lower costs and increasing integration.

Some example products which may be provided with this specification include:

- Advanced Cordless Phone – With a moderate phone display, the user may lookup dialing information from a local address book or from an internet-based white pages. Alternatively, voice recognition may be used to dial numbers and perform lookups. While in a call, an automated assistant using voice synthesis may subtly indicate that an important E-mail from your spouse has arrived. Pausing the phone call, you may see the message on the phone display, and if needed, immediately place a second call. Furthermore, vociemail and email servers on the desktop PC now have the ability to indicate that they have messages waiting by flashing a light on the cordless phone.
- Handheld Browsers – A small device, similar to today's WinCE and Pilot devices, may be used for wireless access to local and Internet information. Review of news stories,

broadcast entertainment listings, as well as interactive content may be performed in any location of the house. Because the information is presented in a comfortable, appropriate manner, the use of customized information delivery services may significantly increase. Because the complexity of the system is low, special function browsers may be created. Digital recipe books may look up cooking information from local and Internet sources. Remote controls may display the current issue of TV Guide™. An email peripheral may also serve as an electronic Post-It™ note with reminders and tasks listed.

- Children's Toys – Both interactive gaming and unique edutaiment devices may reach kids (and adults) who hesitate to sit down before a computer screen. With wireless access to information sources, these devices have a depth, flexibility, and dynamic characteristics beyond what is currently available. For example, an educational toy may present questions based on current news topics, or may be linked to a recently broadcast program. As the curiosity of the child changes in direction, the device may use different approaches to entertain and educate.
- Multimedia Environments – Wireless connectivity to speakers, printers, audio sources also enables new products, such as digital audio players with access to digital content on the internet. The ability to drive printers wirelessly from any of the wireless devices in this network, such as the handheld browsers, children's toys, digital cameras, and

other devices provide an ease of use and convenience by eliminating the various cables currently required.

Operation in the 2.4 GHz ISM band offers the advantage of allowing products to be produced and marketed worldwide with only a few restrictions on power level and channel access methods. However, operating in this freely available band is not without consequences. Consumer microwave ovens radiate a considerable amount of energy in this band. As a result, effective wireless protocols for this band must take this into account.

The microwave oven interference will limit the achievable throughput in this system. Careful examination of the interference waveforms indicates that the microwave is not radiating power all of the time. Since the klystron is active only when the voltage of a half-wave rectified AC power input is greater than some value, interference is only present in a given 1 MHz channel for 40% or less of the time, with a periodic 60/50 Hz cycle. Depending on the center frequency of the channel, some interference patterns appear as two short spikes (702) at the turn on or off points of the klystron. A spectrum analyzer screen capture shown in FIG. 7, numeral 700, illustrates the interference modes that are commonly seen.

To take advantage of this periodic interference, the DA-TDMA protocol operates in the gaps between interference

bursts. The small block size enables transmission of several blocks between the bursts of microwave interference. When the interference is present, error detection CRCs and a fast ARQ enable the system to repeat blocks to maintain reliable, low error rate links. An illustration of this operation is seen below. Because the interference from the microwave may persist for some time, isochronous traffic will need to be buffered because communications may be interrupted for up to 6 milliseconds.

From the start, DA-TDMA was designed to meet the goals of low complexity and high performance while using frequency hopping in the 2.4 GHz band with microwave interference. The combination of a small block size, time division duplexing, and stop-and-wait ARQ achieve these goals and enable significant system throughput. The small block size (.75 milliseconds) easily utilizes the interference free time on the channel. Time Division Duplexing (TDD) will allow the bandwidth to be dynamically allocated between uplink and downlink directions. A central scheduler efficiently allocates bandwidth to isochronous and asynchronous connections. Stop and wait ARQ provides a simple, effective method to provide reliable transmission of the bursts in a low complexity realization.

An illustration of the frame and block diagrams is shown in FIG. 8, numeral 800. Each square in the frame diagram represents a unit of transport, called a block. Each frame lasts for 24 milliseconds, and contains 32 block times. Each frame

is transmitted on a single frequency, and during the 32nd block, the frequency is changed (or hopped) to the next channel. The channel data rate is 1.544 Mbps. Each block can sustain a 32 kbps throughput, yielding a .992 Mbps system throughput. In the presence of microwave interference, sustainable throughput is expected to be 512 kbps or greater. Up to 384 kbps may be reasonable assigned to isochronous traffic, with the remainder being available to asynchronous traffic.

Each block is 0.75 msec long and contains a block assignment, block data, and block acknowledgment. The block assignment is transmitted by the scheduler with synchronization and addressing information to direct the appropriate wireless peripheral to transmit or receive during the payload and acknowledge times. The block payload contains a synchronization word, system control header, sequence number, and 96 bytes of payload. The block acknowledge field represents the outcome of the reception of the payload (positive/negative) and the sequence number from the block data. A 32 microseconds guard time between these block elements minimizes the RF cost by allowing reuse of receiver and transmitter elements.

The scheduler will automatically retry blocks which do not receive a positive acknowledgment. The short packets that overlap microwave interference will be detected and the blocks repeated. In this environment, the ARQ is more efficient

than Forward Error Correction (FEC). FEC consumes bandwidth regardless of the interference environment and would probably not be effective in the presence of significant interference in this system. By contrast, ARQ allows only retries blocks which are corrupted by interference, and provides higher throughput during the majority of time that the channel is clear. ARQ is also lower complexity than FEC, needing no special, complex encoder/decoder.

A scheduling algorithm manages isochronous traffic to provide best-effort delivery in a prearranged time. Using sequence numbers contained in the block data and acknowledgment fields, the scheduler assures that the blocks are transmitted in order, making the reassembly task simple. The minimum scheduling interval is 24 msec. As a result, isochronous data streams will incur a 24 msec buffering delay. Polling is the primary method for transferring information between the base controller and the wireless terminals. This enables very low cost, low power terminal devices. Terminals with a very low demand for informationmay be scheduled for infrequent polling at multiples of the 24 msec polling interval. Alternatively, un-utilized slots may be marked for contention access to allow terminal registration and for data transfer requests initiated by the terminal. Upon receiving a data transfer request, the central controller schedules a poll to the terminal.

The protocol stack builds on both of the fundamental isochronous and asynchronous services provided by the microwave avoidance scheme and borrows heavily from existing standards for the higher layers. FIG. 9, numeral 900, illustrates the In-Home RF Bus protocol stack. At the physical layer (902), a low complexity modulation scheme is employed to provide for low-cost modem designs. Differential QPSK has been identified operating at 1.544 Mbps providing for 32 32-kbps isochronous block in a 24 ms frame. Each block in the frame is indistinguishable from the next, further reducing the complexity of the modem. These blocks are the fundamental pieces of the fast-packet ARQ scheme used to avoid microwave interference. Frequency hopping has been super-imposed on top of the frame/block structure in order to comply with FCC regulation for high-power operation and provide multi-user protection in high density urban environments. The system hops at a moderate rate, once every frame (24 ms), allowing for fast synchronization of new devices but without requiring fast synthesizer switching times (<750 ms). One of the 32 blocks is reserved for synthesizer switching every frame.

The datalink layer (904) implements the microwave avoidance scheme. Unacknowledged blocks are retried until successfully acknowledged or dropped based on criteria of the service being delivered. For isochronous services each block is retried for the duration of an Isochronous Window (IW) which is a period of 24 ms beginning at a particular block in a frame and ending at that same block in the succeeding frame. The

limited retry duration bounds the delay to a finite level. For end-to-end synchronous services the receiver may insert dummy bits to maintain bit-count integrity resulting in a information bit-error rate. However, dropped blocks are expected to be very low and error mitigation techniques should allow for a high-quality of service. For asynchronous services each block may theoretically be retried indefinitely since the delay is less critical for these devices. However, practical concerns require a cap, albeit high, be placed on the number of asynchronous retries to handle aberrant events when a peripheral device is out-of-range or shadowed. In an error-free environment 31 32-kbps blocks per frame provide 992 kbps user throughput. At microwave interference duty-cycles of 40% a 512 kbps user throughput may still be realized.

At the network layer (906), two classes of protocols are defined a Native Protocol (NP) and the Internet Protocol (IP). The NP is intended for the lowest cost devices such a cordless phone with simple numeric displays, wireless extension of parallel/serial ports, or integrated home appliances. Often, devices using NP are fundamentally isochronous and require a low amount of associated data traffic. For example, a cordless phone would only need to communicate key presses to the serving application and receive updates to the alpha numeric display. In other cases, such as a parallel or serial port extender, the device's overlaying data protocol is rudimentary and may be handled in a simple block by block transfer.

For more sophisticated devices such as laptops and a generic information appliance, IP has been adopted to build on the established base of protocols and provide a familiar API to the developer. To support IP, several services are incorporated into the datalink layer (904). A fragment/reassembly service is required to aggregate the physical blocks of 96 octets each into asynchronous packets capable of carrying the typical IP MTU of 1500 octets. The standard Point-to-Point Protocol (PPP) will reside on top of the asynchronous packets providing for the encapsulation of IP packets and may allow the extension of services to other network protocols in the future. Most importantly, PPP provides a well documented procedure for negotiating network layer connectivity including the options of assigning dynamic IP addresses and using IP header compression. Other supporting datalink services include IP switching and Network Address Translation (NAT). IP switching is required since logically the network appears as a star configuration with point-to-point links, provided by PPP, to each peripheral device. The base station in this case will be required to map IP address destined for pier device to the physical address of that device. Unlike, traditional Local Area Networks (LANs) the physical address will be hidden from the IP stack eliminating the need for costly broadcast packets used by protocols such as the Address Resolution Protocol (ARP) which maps physical addresses to IP addresses in each client device. The NAT protocol, also referred to as "IP masquerading" , will enable the IP administration process to

be completely transparent to users and provide compatibility with existing Internet Service Providers (ISPs). The NAT protocol provides an address translation between IP addresses/Port Numbers on a private network to those on the Internet at large. Therefore, an in-home network will present one address to the Internet while maintaining multiple private addresses for the various local wireless peripherals. The split in addressing allows in-home networks to duplicate addresses from one private network to the next without over burdening global Internet and requiring that each consumer obtain a set of IP addresses. Furthermore, one global address is consistent with the services currently being offered by ISPs.

The following defines the minimum requirements for devices which inter-operate on the In-Home RF Bus air-interface. The System Architecture provides a functional reference diagram for the system defining the terms for the various devices and interfaces. The Physical Layer (Layer 1) defines the channelization, modulation, frame/block/burst structure, inter-system inference protection and RF transceiver requirements. The Datalink Layer (Layer 2) specifies the multiple access, ARQ procedures, connection establishment, and data transport procedures. The Network Layer (Layer 3) defines the registration, de-registration and service negotiation procedures.

The architecture of the In-Home RF Bus protocol is defined in terms of interfaces, devices, applications, and connections.

The interfaces refer to the physical media over which the data is communicated. Devices define the end-points of the various interfaces. The applications furnish the services provided to registered peripherals. Connections carry the data between a registered peripheral and the serving application.

The In-Home RF Bus functional reference architecture is depicted in FIG. 10, numeral 1000. It defines five types of devices--Legacy Peripherals (1002), Wireless Peripherals (1004), Wireless Access Points (1006), Computational Resources (1008), and Wired Voice & Data Networks (1010)—and four interfaces—the Legacy (L), Air (A), Computational (C), and Network (N).

Legacy peripherals (1002) cover all devices that have traditionally been wired to a computer such as printers, scanners, and laptops. These devices may be connected by an emulated wired interface carried over the A-Interface to the personal computer . This emulated interface is referred to a the L-Interface or Legacy-Interface. The L-interface may be a PCI, RS-232, ISA, or Parallel Port.

Wireless peripherals (1004) cover all devices that have an integral RF component. These devices may include a advanced cordless phone, an information appliance, or a data adapter to a legacy device. Wireless peripherals communicate in the 2.4 GHz ISM band to centralized controller called the Wireless Access Point. The wireless peripheral employs applications

offered by the wireless system which may be provided at the computational resource, the wired voice and data network, or the Wireless Access Point.

The Wireless Access Point (1006) or simply access point manages the communication link, coordinating the transmission of all wireless peripherals and providing access to both the computational resources and the network. The access point connects to the computational resource over the C-Interface. This C-Interface may take the forms of a USB, PCI, ISA, or Device Bay. Alternatively, the C-Interface may be maintained over the wireless A-Interface to wirelessly connected computer. In either case, the access point manages access to the computational resource and is aware of all available applications. In addition, the access point may also maintain a connection to wired voice & data network over the N-interface. The N-Interface may take on the forms of a POTS modem, ADSL, ISDN, or Cable.

The wired voice & data network (1010) represents a connection to the Public Switched Telephone Network, the Internet, a cable provider, or satellite network.

This description only defines the operation of the A-Interface. It specifies how wireless peripherals communicate with access points and how these wireless peripherals connect to applications. It ensures interoperability between access points and wireless peripherals created by different

manufacturers allowing consumers to buy equipment from multiple sources. It does not dictate the architecture of devices or applications.

For the purposes of this description, Legacy peripherals connected to data ports will not be distinguished from integrated wireless peripherals. The term "peripheral" will refer to both.

All services utilized by peripherals on the In-Home RF Bus are managed by applications. Applications may reside in the access point, the personal computer, a wired network device, or wirelessly connected device. Moreover, applications may be distributed across multiple devices with each device providing a specialized function that enhances the overall application. For example, a POTS application provides connectivity to the PSTN but may also rely on the personal computer for voice enhanced features and the Internet for directory look-up. The peripheral, however, perceives all applications and their features to reside within the access point. The access point is responsible for maintaining this appearance and must coordinate a peripheral's connection to a distributed application.

FIG. 11, numeral 1100, shows a Logical Reference Architecture that illustrates the conceptual architecture of an access point. Each line in the figure denotes the logical connections in the system. Each logical connection on the A-

Interface corresponds to a unique physical layer sub-address (see below with respect to Addressing). At initial system access, all peripherals (1102) are given a default logical connection, called the "control connection", to the access point's (1108) Device Management Function (DMF; 1104). The DMF is a special application responsible for maintaining radio link with all peripherals and managing all subsequent connections within the system. Furthermore, the DMF must account for all applications (1106) in the system routing application specific information transmitted on the control connection to the appropriate application.

The control connection provides the fundamental link for a peripheral to access services form the system. At initial system access, a peripheral will first register with the DMF and then begin a service negotiation phase which registers it with each individual application. The registration and negotiation all take place on the control connection. Additional connections, called "direct connections", may be assigned to the peripheral during the registration process or alternatively these connections may be assigned dynamically at a later time. FIG. 12, numeral 1200, illustrates a direct connect (1202) between a peripheral (1204) and an application (1206). These direct connections are used to carry application data which is interpreted solely by the application running in the access point and the application's client running in the peripheral. The format of application data is unique to the application. Typically, all asynchronous direct connections

are assigned during the registration process while all isochronous direct connections are assigned dynamically. The control connection is always maintained.

Peripherals that wish to connect to the wired voice and data network must always go through an intermediate application. Two default applications are defined for this purpose, the POTS application and the PPP application.

The POTS application connects advanced cordless phones and similar peripherals to the PSTN making use of isochronous connections in the system. As shown in FIG. 13, numeral 1300, to illustrate how connections may be assigned, it useful to examine how an incoming call is handled by the system. FIG. 13 (a; 1302) illustrates a system with three cordless extension phones. When a incoming call arrives from the PSTN, the POTS application pages each connected peripheral in the system via the DMF over the control interface. The DMF is aware of the standby mode of each peripheral and transmits the page when the device is listening. In the example, two people pick up two different peripherals to answer the call. These two peripherals send an off-hook indicator on the control interface along with a request for a direct isochronous connection to the application (b; 1304). Upon connecting, the application would sum the audio from both peripherals and route the composite audio signal to the PSTN (c,; 1306). At the end of the conversation, an on-hook indicator is sent on the control interface by both peripherals requesting the direct isochronous

connection to be discontinued (d; 1308). The DMF would interpret a portion of the on-hook indicator and terminate the direct isochronous connections.

The PPP application connects information appliances and similar devices to the wired data network and provides IP connectivity to local peripherals. The PPP application is based on the Internet Standard RFC 1661 'The Point-to-Point Protocol" and treats peripheral's direct connection to the PPP application as a dedicated point-to-point connection. The PPP application terminates all PPP connections and therefore must understand the network protocols encapsulated. At a minimum, a compliant PPP application must support the Internet Protocol (IP). IP can be used to connect the peripheral to the Internet at large, or simply, two peripherals over the A-Interface. For example, two laptop computers may be networked using IP. Unlike the POTS application, the PPP application assigns its direct connections during the service negotiation phase. Once assigned, the PPP connection is maintained indefinitely. The DMF participates in an asynchronous transfer and is responsible for allocating bandwidth for uplink traffic and scheduling downlink traffic with respect to standby modes. On the uplink, the initial block of asynchronous transfer is transmitted over the control connection containing the length of the transfer and address of the connection. Since the connection has already been established at registration, the DMF can quickly route the data to the PPP application and allocate the bandwidth as requested on the direct PPP

connection. Likewise on the downlink, the initial block is transmitted over the control connection during a paging interval to announce an impending packet. Once the peripheral is known to be listening, the remainder of the transfer is transmitted on the direct PPP connection

The precise addressing of connections is defined below. Addressing. .Isochronous and Asynchronous connections as well the registration process are defined in below with respect to Connections.

The A-Interface operates in the 2.4 GHz ISM band employing a form of Dynamic Acknowledged-Time Division Multiple Access (DA-TDMA) and Time Division Duplexing (TDD). Unlike traditional TDMA, the system dynamically assigns blocks of time as opposed to the periodic assignment of blocks into timeslots. Furthermore, each block is immediately acknowledged. Both Isochronous and Asynchronous traffic is supported. The maximum data-rate provided to either traffic is 992 kbps with a fundamental data-rate of 32 kbps. Slow-frequency hopping is used to mitigate inter-system interference hopping at a rate 41.67 hops per second.

This description defines the details of the physical layer. The Channel Access Strategy defines the Channelization of the ISM band the modulation technique. The 3.2.2 Frame and Block Structure defines the format of the DA-TDMA/TDD channel. The Multi-System Interference details the frequency hopping

method, scrambling, and color coding. The RF Transceiver Requirements defines the minimum requirements of the transceiver including sensitivity and spurious emissions.

The A-Interface divides the ISM band into 95 1 MHz channels with each channel carrying a 1.544 Mbps modulated signal.

Channels are numbered from 0 to 94. Channels are 1 MHz wide with centers spaced 1.0293 MHz (exactly 2*1.544/3 MHz) apart. The center of channel 0 is at 2401.6919 MHz (exactly 9333*1.544/6 MHz). The center frequency for channel n is given exactly by the following formula:

$$f(n) = \frac{1.544}{6}(4n + 9333) \text{ MHz} \qquad 0 \le n \le 94$$

In most countries regulations exist which allow only a subset of these channels to be used. See the description on frequency hopping for details regarding the use of channels.

Both the access point and the peripheral employ p/4 shifted differential quadrature phase shift keying (p/4-DQPSK) modulation. A full raised cosine pulse shaping filter shall be employed with a bandwidth expansion factor of 0.25. A block diagram of the modulator is shown in FIG 14, numeral 1400

The serial-to-parallel converter (1402) accepts a serial bit-stream and converts this to the bit sequence pair X_k, Y_k where X_k is formed from the odd numbered bits of each field

and Yk is formed from the even numbered bits. The first bit of each field is bit 1 and is therefore an odd bit. The differential encoding unit (1404) performs differential encoding as:

$$I_k = I_{k-1}\cos[\Delta\Phi(X_k, Y_k)] - Q_{k-1}\sin[\Delta\Phi(X_k, Y_k)]$$
$$Q_k = I_{k-1}\sin[\Delta\Phi(X_k, Y_k)] + Q_{k-1}\cos[\Delta\Phi(X_k, Y_k)]$$

Symbols are transmitted with the phase changes shown in Table 1, which defines DF in the above equation .

Table 1 Modulator phase transitions for all input patterns.

X_k	Y_k	$DF(X_k, Y_k)$
0	0	+p/4
0	1	+3p/4
1	1	-3p/4
1	0	-p/4

The impulse sequences I_k and Q_k are filtered by a linear phase Nyquist pulse shaping filter to form the continuous signals i(t) and q(t). The filter shall be a full raised cosine filter with a

25% bandwidth expansion factor. The frequency response for this filter is given by:

$$|H(f)| = \begin{cases} 1 & |f| < (1-\alpha)/2T \\ \frac{1}{2} * (1 - \sin[(2fT-1)p/2\alpha]) & (1-\alpha)/2T < = |f| < (1+\alpha)/2T \\ 0 & |f| = > (1+\alpha)/2T \end{cases}$$

where T is the symbol period and a is the bandwidth expansion factor of 0.25.

The transmitted signal s(t) is derived from i(t) and q(t) through quadrature modulation of a carrier given by the following:

$$s(t) = i(t) * \cos(\omega_c t) - q(t) * \sin(\omega_c t)$$

where w_c is the RF carrier frequency. The channel bit rate of 1.544 megabits per second corresponds to a symbol rate of 772 kilosymbols per second.

The DA-TDMA/TDD channel is sub-divided into blocks of time called transa burst which is broadcast by the access point to all peripherals in the system. The second burst is the Payload burst which is transmitted by either a peripheral or the access point. The last burst is the Acknowledgment/Sequence Number (ACKSEQ) which, when transmitted, is transmitted by the peripheral. Thirty-two transaction blocks are grouped into a 24 millisecond frame. Frames are number from 0 to 524287.

Transaction blocks are number from 0 to 31. FIG. 15, numeral 1500, Frame, Block, and Burst Formats. illustrates the DTDMA/TDD format. The fields within the Block Assignment Burst, Payload Burst (1502) and Acknowledgment/Sequence Number burst (1504) are defined below.

The BA burst enables the dynamic allocation and duplexing features of the DTDMA/TDD channel, assigning both the source and destination device at the beginning of each block transaction. The source and destination address fields may either specify an access point or peripheral enabling downlink (access point to peripheral), uplink (peripheral to access point), or pier-to-pier (peripheral to peripheral) transfers. In addition, the BA field contains general broadcast information to identify the system, the current transaction block, the current frame, and the RF channel of the next frame. Finally, the acknowledgment value, received from the destination peripheral in the previous frame, is repeated as part of the BA field. The addresses, broadcast information, and acknowledgment fields are all protected by a 24-bit CRC. Furthermore these protected fields are preceded by differential encoding reference symbol (2-bits) and a synchronization word (32-bits). Table 2 defines the order and the content of the fields within the BA burst.

Table 2 Block Assignment Burst Fields

Fields	Description	Bit Indices (begin/end)		Length
Differential Encoding Reference Symbol	Provides a reference for the differential modulation.	0	1	2 bits
Synchronization Word	The sync word is the following binary value %00000101111101011100100111000110.[1]	2	33	32 bit
Block Count	Specifies the number of the current block. It is incremented sequentially for each new frame taking on the values 0 through 31.	34	34	5 bits
Frame Count	Specifies the number of the current frame. It is incremented sequentially for each new frame taking on the values 0 through 524287. It will not repeat for at least 3.5 hours.	35	46	19 bits

Acknowledgment	Status of the transfer in the previous transaction block. Set to 1 if it was successful and set to 0 if it was not.	47	58	1 bit
Next Frequency	Specifies the channel of the next frame.	59	66	7 bits
System ID	A short ID, selected by the access point upon power-up, used to distinguish the system from it's neighbors.	67	85	8 bits
Source Address	The address of the source device and respective connection.	86	90	12 bits
Destination Address	The address of the destination device and respective connection.	91	97	12 bits
Reserved	Reserved field must be encoded as 0.	98	107	10 bits
CRC	See Section 3.2.2.2 Error Detection	108	131	24 bits

[1] The maximum sidelobe of the out-of-phase auto-correlation and the merit factor, a function of the sum of the squares of the out-of-phase auto-correlation, are commonly used to determine good synchronization words. The binary sequence %00000101111101011100100111000110 minimizes the maximum sidelobe and maximizes the merit factor over all 32-bit sequences, where only even (symbol) phase auto-correlation are considered.

The Payload burst carries both the control and user information in the system. The preceding BA burst specifies the source and destination device. The source device transmits the payload burst while the destination device receives it. The payload burst is 838 bits long and carries a 768 bit (96-octet) data field for control and user information. The data field is preceded by a header field made up of a System ID, Scramble Mode, Control Connection Status, Reserved bits, Sub-address Block Sequence Number (SBSN), and Extended Header Indicator. Bursts sent on the control connection extend the header by 4 octets into the data field. The control connection extended header is defined in section 3.3.1.2. The header and data fields are protected by a 24-bit CRC. Like the BA burst, the protected fields are preceded by a differential reference symbol and synchronization word. Table 3 defines the order and the content of the fields within the payload burst.

Table 3 Payload Burst Fields

Fields	Description	Bit Indices (begin/end)		Length
Differential Encoding Reference Symbol	Provides a reference for the differential modulation.	0	1	2 bits
Synchronization Word	The sync word is the following binary value %00000101111101011100100111000110.	2	33	32 bit
System ID	A short ID identical to the field in the previous BA burst.	34	41	8 bits
Scramble Mode	Specifies whether the remaining fields in the burst are scrambled by a pseudo random sequence. A value of 1 indicates that the fields are scrambled.	42	42	1 bit

Control Connection Status	Specifies whether the source peripheral requires a control block. A value of 1 indicates a control message is pending. This field is not valid when the source device is an access point.	43	43	1 bit
Reserved Bits	Must be encoded as 0.	44	44	4 bits
SBSN	Sub-address Block Sequence Number	45	48	1 bit
Extended Header	Indicates that the header is extended into the payload using the 3-octet control connection extended header format. A value of one indicates the header is extended. See section 3.3.1.2 Control Connection Extended Header.	49	49	1 bit
Data	96 octets of user data on dedicated connection. (92 octets on a control connection.)	50	817	768 bits
CRC	See Error Detection	818	841	24 bits

The ACKSEQ burst communicates the status of payload transfer to a peripheral by sending a 32-bit codeword from the peripheral to the access point. For a given system, the codeword can take on the three values ACK-0, ACK-1, or NAK. ACK-0 and ACK-1 correspond to successful transactions, with

ACK-0 if the SBSN of the acknowledged payload equaled 0 or ACK-1 if the SBSN equaled 1. If the transfer was not successful, the peripheral transmits a NAK. A NAK is transmitted instead of no response so the receiver will not mistake random noise for an ACK. The access point then uses the ACKSEQ information in it's scheduling algorithm to ensure that appropriate blocks are assigned per connection. The value of the acknowledgment, ACK or NAK, is repeated in the BA burst in the following transaction block.

Between systems, the encoding of the ACKSEQ codeword is colored based on the 5 least significant bits of the System ID defined in the description for Color Coding below. Color coding is used to combat the rare occurrence of an access point interpreting an ACKSEQ burst from a neighboring system's time and frequency aligned peripheral as an ACK from an actively communicating peripheral that went out of range or is momentarily shadowed. 32 color codes ensure that all nearest neighbors can have a different color code.

When the System ID is set, both the access point and peripheral compute and store the ACK-0 and ACK-1 codewords. The access point compares these codewords to the received data to determine if an ACK was received. The peripheral also computes and stores the NAK codeword, and sends ACK-0, ACK-1 or NAK as appropriate. Devices only need to recompute the codewords when the System ID is changed.

The three codewords for each color code are given in Table 4 below. Each codeword is immediately preceded by a differential encoding symbol.

5

Table 4 ACKSEQ Codewords

Color Code	ACKSEQ	
0	SEQ-0	11000000110100001010011011111101
	SEQ-1	10000000100111110011101101010110
	NAK	01000000010011111001110110101011
1	SEQ-0	10101110101101111000001100000001
	SEQ-1	11101110111110000001111010101010
	NAK	00101110001010001011100001010111
2	SEQ-0	00011100000111101110110100000101
	SEQ-1	01011100010100010111000010101110
	NAK	10011100100000011101011001010011
	SEQ-0	01110010011110011100100011111001

3	SEQ-1	0011001000110110010101010 10010
	NAK	1111001011100110111100111010 01111
4	SEQ-0	0111100001110010010001111010 00001
	SEQ-1	0011100000111101110110100000 01010
	NAK	1111100011101101011111001111 10111
5	SEQ-0	0001011000010101011000100101 11101
	SEQ-1	0101011001011010111111111111 10110
	NAK	1001011010001010010110010000 01011
6	SEQ-0	1010010010111100000011000101 11001
	SEQ-1	1110010011111001110010001111 10010
	NAK	0010010000100011001101110000 01111

7	SEQ-0	1100101011011011001010011010100101
	SEQ-1	1000101010010100101101000000001110
	NAK	0100101001000100000100101111010011
8	SEQ-0	1011000010101011000100101110101001
	SEQ-1	1111000011100100100011110100000010
	NAK	0011000000110100001010011011011111
9	SEQ-0	1101111011001100001101110001010101
	SEQ-1	1001111010000011101010101011111110
	NAK	0101111001010011000011000100000011
10	SEQ-0	0110110001100101010110010001000101
	SEQ-1	0010110000101010110001001011011010

	NAK	11101100111111010011000100100111
11	SEQ-0	00000010000000100111110011101101
	SEQ-1	01000010010011011110000101000110
	NAK	10000010100111010100011110111011
12	SEQ-0	00001000000010011111001110110101
	SEQ-1	01001000010001100110111000011110
	NAK	10001000100101101100100011100011
13	SEQ-0	01100110011011101101011001001001
	SEQ-1	00100110001000010100101111100010
	NAK	11100110111100011110110100011111
	SEQ-0	11010100110001111011100001001101

14	SEQ-1	10010100100010000010010111100110
	NAK	01010100010110001000001100011011
15	SEQ-0	10111010101000001001110110110001
	SEQ-1	11111010111011110000000000011010
	NAK	00111010001111111010011011100111
16	SEQ-0	00100000001001111100111011010101
	SEQ-1	01100000011010000101001101111110
	NAK	10100000101110001111010110000011
17	SEQ-0	01001110010000001110101100101001
	SEQ-1	00001110000011110111011010000010
	NAK	11001110110111111101000001111111

18	SEQ-0	11111100111010011000010100101101
	SEQ-1	10111100101001100001100010000110
	NAK	01111100011101101011111001111011
19	SEQ-0	10010010100011101010000011010001
	SEQ-1	11010010110000010011110101111010
	NAK	00010010000100011001101110000111
20	SEQ-0	10011000100001010010111110001001
	SEQ-1	11011000110010101011001000100010
	NAK	00011000000110100001010011011111
21	SEQ-0	11110110111000100000101001110101
	SEQ-1	10110110101011011001011111011110

	NAK	01110110011111010011000100100011
22	SEQ-0	01000100010010110110010001110001
	SEQ-1	00000100000001001111100111011010
	NAK	11000100110101000101111100100111
23	SEQ-0	00101010001011000100000110001101
	SEQ-1	01101010011000111101110000100110
	NAK	10101010101100110111101011011011
24	SEQ-0	01010000010111000111101011000001
	SEQ-1	00010000000100111110011101101010
	NAK	11010000110000110100000110010111
	SEQ-0	00111110001110110101111100111101

25	SEQ-1	01111110011101001100001010010110
	NAK	10111110101001000110010001101011
26	SEQ-0	10001100100100100011000100111001
	SEQ-1	11001100110111011010110010010010
	NAK	00001100000011010000101001101111
27	SEQ-0	11100010111101010001010011000101
	SEQ-1	10100010101110101000100101101110
	NAK	01100010011010100010111110010011
28	SEQ-0	11101000111111110100110111001111101
	SEQ-1	10101000101100010000011000110110
	NAK	01101000011000011010000011001011

29	SEQ-0	1000011010011001101111100111 00001
	SEQ-1	1100011011010110001000111101 01010
	NAK	0000011000000110100001010011 10111
30	SEQ-0	0011010000110000110100000111 00101
	SEQ-1	0111010001111111010011011101 01110
	NAK	1011010010101111111010110011 10011
31	SEQ-0	0101101001010111111101011001 11001
	SEQ-1	0001101000011000011010000011 10010
	NAK	1101101011001000110011101101 01111

The codewords are generated by systematically encoding the seven information bits given in Table 5 below. Bits 6 and 5 are created such that no all 0 or all 1 ACKSEQ bursts are formed.

5

Table 5 Information bits that are systematically encoded to form the ACKSEQ.

Bit	Source
0	SYSTEM ID bit 0
1	SYSTEM ID bit 1
2	SYSTEM ID bit 2
3	SYSTEM ID bit 3
4	SYSTEM ID bit 4
5	1 for NAK, 1 for SEQ-0, 0 for SEQ-1
6	1 for NAK, 0 for SEQ-0, 1 for SEQ-1

The information bits are mapped to the ACKSEQ bits as shown in Table 6, where '+' stands for exclusive or.

Table 6 ACKSEQ generation table.

ACKSEQ Bit	XOR of Information Bits
0	5
1	6
2	6+5+3+2+0
3	5+4+2+1+0
4	6+5+3+2+1+0
5	5+4+1+0
6	6+5+2+1+0
7	5+1+0
8	6+2+1+0
9	6+5+1
10	5+3+0
11	6+4+1
12	6+3
13	6+5+4+3+2+0
14	4+2+1
15	5+3+2
16	6+4+3+0
17	6+4+3+2+1+0

18	6+4+1+0
19	6+3+1
20	6+5+4+3
21	4+3+2+0
22	5+4+3+1+0
23	6+5+4+2+1
24	none (always equals zero)[1]
25	0
26	1+0
27	2+1+0
28	3+2+1
29	4+3+2+0
30	5+4+3+1+0
31	6+5+4+2+1

[1] While this bit may be removed without affecting the minimum distance of the code, it is left as is to have an even number of bits for the QPSK modulation. It is not made a function of the information bits because the cyclic nature of the code would be lost.

The mapping in the table is equivalent to systematically encoding (See Lin and Costello p. 95. with the (37,7) shortened cyclic code generated by

$g(x)=1+x^8+x^{11}+x^{12}+x^{13}+x^{14}+x^{15}+x^{18}+x^{19}+x^{20}+x^{22}+x^{23}+x^{25}+x^{27}+x^{29}+x^{30}$

and removing the 5 bits associated with the color code. This code is an optimal (37,7) code, with a minimum distance of 16. No other (37,7) code can have a greater minimum distance (See A. E. Brouwer and T. Verhoeff, "An Updated Table of Minimum-Distance Bounds for Binary Linear Codes," *IEEE Trans. Inform. Theory*, vol. IT-39, pp. 662-677, March 1993. Creating the ACKSEQ codewords with this optimal code gives us the following properties:

1. Because of the cyclic nature of the code, single bit shifts of a codeword will differ in at least 14 positions from the other codewords, making the ACKSEQ very robust to timing uncertainty.
2. With no multi-system interference, a NAK and an ACK differ in at least 16 positions. A NAK can have up to 7 bit errors in 32 bits and still not be misinterpreted as an ACK, and vice-versa.
3. With no multi-system interference, ACK-0 and ACK-1 differ in at least 16 positions, and at least 7 bit errors can be corrected out of 32 bits.
4. With multi-system interference, an ACK or a NAK from another system will differ from the present system's ACK in at least 11 positions. Therefore, an ACK from another

system cannot possibly be accepted unless there are more than 5 bit errors out of 32 bits.

5. In 50% BER conditions (microwave interference, portable out-of-range, multi-system collision) the 32 bit ACKSEQ can provide up to 31 bits of random noise protection, depending on the amount of error correction desired.

The CRC codes used for detecting errors in the BA and Payload packets are essential to the ARQ protocol, as described below with respsect to ARQ protocol and scheduling. A poor choice of CRC generator polynomial can lead to erratic behavior in the source, destination, and scheduler state machines due to undetected errors. Very long CRC codes, with good generator polynomials, can limit undetected errors, but consume bits in the air interface and can cause throughput problems due to false alarms. By keeping the length of the CRC as small as possible while providing adequate error detection, and by handling any undetected errors that do occur in the ARQ protocol gracefully, these problems can be avoided.

A 24-bit CRC is used to protect 74 bits of the BA (bits 34 to 107), and another 24-bit CRC is used to protect 784 bits of the Payload (bits 24 to 817). Both CRCs are implemented with the same generator polynomial $g(x)=1+x^2+x^3+x^4+x^5+x^7+x^8+x^{16}+x^{17}+x^{19}+x^{20}+x^{21}+x^{22}+x^{24}$(A textbook reference implementation for a CRC is given on page 95 of Lin and Costello.)

This CRC has very good minimum distance properties. (G. Castagnoli, S. Brauer, and M. Herrmann, "Optimization of Cyclic Redundancy-Check Codes with 24 and 32 Parity Bits," *IEEE Trans. Commun.*,vol. COM-41, pp.883-892, June 1993.

FIG. 16, numeral 1600, below shows the probability of BA (1602) and Payload (1604) bursts having an undetected error, for a range of error conditions. The CRC codes at this length are considered proper because the undetected error curve is non-increasing for decreasing bit error rate. (CRC codes are not guaranteed to be proper, so any candidate generator polynomial needs to be verified for each number of bits it may protect.

The results are more than adequate at the specified nominal operating point of 10^{-5}. In random noise conditions, such as that seen by the Access Point when no peripherals are present, noise will not be accepted as a block unless it passes the 32-bit synchronization word, matches the 8-bit System ID, and passes the 24-bit CRC.

The BA, Payload, and ACKSEQ bursts will all be separated in time by a 50 symbol (32.38 microsecond) guard band. Without accounting for propagation delay, the guard band shall be accurate within +/- one symbol time.

Multi-System Interference

This system will be able to operate in dense urban environments such as apartment buildings and multi-family dwellings. In order to operate effectively in these environments, a variety of multi-system interference mitigation methods are used. Frequency hopping will reduce the likelihood that neighboring systems utilize the same channel for an extended period of time. Scrambling and color coding will minimize the risk that systems that happen to be using the same channel at a given time will misinterpret channel data. However, no coordination between neighboring base stations is required. As a result, there will always remain a slim chance that adjacent systems will choose the same values. If a system detects that it is receiving interference from a system with the same color code, scrambling code or frequency hopping pattern, it may choose to restart with different choices of frequency hopping pattern, scrambling sequence and color code. Peripherals would then need to re-register and obtain these new values. This should not be done lightly, as currently active links will be interrupted as the devices reacquire.

In order to operate in the presence of other systems, each access point randomly selects a frequency hopping pattern (FHP) from a set of FHPs. Each of the K FHPs in the set is of length N, and each element of the FHP is an index to one of q frequency channels. All units in the system switch channels (hop) at the end of each frame based on the FHP. The units hop

to a new frequency channel at the end of a frame during the last block of the frame, block 32. Since the hopping is occurring during a block time, block 32 cannot be used to transmit information, although the access point still transmits a BA with a null address to aid in system synchronization. The FHP is stepped through until it is exhausted, at which time the pattern is repeated from the beginning. Since FHPs are selected with good correlation properties, two systems using different hopping patterns or a different phase of the same hopping pattern will have limited multi-system interference. In the unlikely event of two systems using the same phase of the same pattern, one or both of the systems may randomly select (based on a serial number) a new FHP from the set of FHPs as described previously The set of FHPs used by the system will vary by region in order to exploit and conform to regional differences in the 2.4 GHz ISM rules. The FHPs have the following desired properties:

1. Use all frequencies in the FHP equally often.
2. Minimize cross- and auto-correlation among patterns (to minimize multi-user interference).
3. Are simple to generate (so base does not have to store an entire set of FHPs).

In addition, the regional rules specify the maximum number of frequency channels and the minimum number of frequencies q that the FHP must hop over.

An example of good FHPs are those generated by Titlebaum's linear congruential method (Edward L .Titlebaum, "Time-

Frequency Hop Signals Part I: Coding Based Upon the Theory of Linear Congruences," *IEEE Transactions on Aerospace and Electronic Systems*, vol AES-17, no. 4, July 1981, pp. 490-493.). These patterns satisfy all the above criteria. For any prime number p, the method easily creates a set of $K=p-1$ patterns of length $N=p$ over $q=p$ frequency channels. For the United States, we select $p=79$, the maximum number of frequency channels that the units can support. In other regions, we can use a subset of these 79 channels by simply specifying an offset and a smaller prime number. In any case, it is expected that manufacturers will jointly agree on sets of hopping patterns that satisfy these criteria, from which the base unit will randomly select one.

Frequency hopping information is communicated through the 8 bit "FH Word" data element contained in every BA. A unit can read the current BA's FH Word to know which channel to hop to at the end of the current frame. This is essential before and during the registration process, because the unit is not synchronized with the base's FHP. At the end of registration, however, the base uses the data packet that accompanies the Registration Acknowledge packet to download the entire FHP into the unit. The unit then does not have to read the BA field every frame to know where to hop to next, and can weather long periods of interference, such as might be expected as the unit goes in and out of range from the base. In addition, the unit can now power down and "sleep" for long periods of time,

awakening on the correct frequency channel by advancing the index into the FHP by the number of frames of sleep.

Sleeping can lead to much improved battery life, as described below in Standby Modes. However, without intelligent frequency hopping management, the unit would have to resynchronize to the FHP through re-registration at the end of each sleep period. With this frequency hopping architecture, units would only have to re-register if the base changes the FHP used by the system, and then only if the individual unit happened to be in a long-term sleep at the time. Units that are awake can compare the received FH Word with the next value in their stored FHP; if the values are different, the unit can update its FHP without fully restarting the registration process.

A summary of the frequency hopping parameters and fields is given in Table 7, Frequency Hopping Parameters.

Table 7 Frequency Hopping Parameters

Parameter/Field	Description	Value (typical U.S.)
q	# of frequency channels	max 128 (79)
N	length of FHP	max 128 (79)
K	# of patterns	max 128 (78)
FH Word	frequency channel, 0..*q*-1	8 bits
FHP	list of frequency channels, indexed 0..*N*-1	*N* * 8 bits

Color coding provides additional protection from accidentally receiving a burst from another system. This field, SYSTEM ID, contains a random number selected by the access point and communicated in every Block Assignment and Block Transfer. This field must be checked to determine if the data is destined for that system. If the SYSTEM ID does not match, the data assumed to be in error regardless of whether the CRC passed. Additionally, it is used to select the acknowledgment codes used with a given system.

Scrambling can be used to enable privacy on the data payload. For each payload where the scrambling is enabled (PN-EN bit in the Payload header is set), a 16 bit scrambling seed (data element PN Seed) is loaded in the scramble PN

generator, and successive outputs of that generator are exclusive-or'ed with the data header (bits 43 to 841) and data payload (all bits). The scrambling seed is set at registration and communicated as part of the registration acknowledge message. The seed is randomly selected and remains constant for a given SYSTEM ID for the base. It should be random with respect to the selection of the frequency hopping pattern and the SYSTEM ID.

The PN generator for the scramble sequence is defined by the primitive irreducible generator polynomial $g(x)=1+x+x^3+x^{12}+x^{16}$. A textbook reference shift register implementation of this generator is shown in FIG. 17, numeral 1700. The 16 bit value Scramble Code Index is loaded into the shift register, and the output is taken as shown for use with the first bit of the scrambled sequence. The shift register is then clocked and the process repeats. Note that there are 65535 different scrambling codes, plus the Scramble Code Index of 0 which corresponds to no scrambling (While more scrambling codes may be provided with a longer shift register, the security would still be considered "Cordless Phone Grade" and no additional performance advantages would be provided.)

This description provides specifications necessary to the design of the RF and IF transceiver sections of the access point and peripheral. First, requirements of the access point and peripheral receivers. are specified.

The receiver shall be able to achieve a packet error rate of less than 1% prior to any correction due to retransmission in the presence of thermal noise when the received signal strength is greater than -80 dBm. A packet error in the peripheral is defined as a CRC failure in either the block assignment or the received payload field. A packet error in the access point is defined as a CRC error in the payload field in a block in which a peripheral transmitted as instructed by the block assignment.

The input third order intercept point of both the access point and peripheral receiver shall be greater than -16 dBm.

The 1 dB compression point of both the access point and peripheral receiver shall be greater than -26 dBm.

The adjacent channel rejection ratio shall be greater than 50 dB for a signal 3 channels removed from the desired and 0 dB for signals in the adjacent channel. Adjacent channel rejection ratio is the highest achievable ratio of power in an adjacent channel to desired signal strength while maintaining the specified BER. The on channel signal is adjusted to a level 3 dB above the minimum specified for a 10^{-5} BER. The unwanted signal level is increased to the lowest level where a 10^{-5} BER of is obtained during the transmission of at least 10^{7} bits. The adjacent channel rejection ratio is the ratio of the desired signal power to the unwanted signal power.

The receiver shall have a spurious response of no greater than 35 dB via the measurement procedure described in EIA document EIA/TIA-204-D "Minimum Standards for Land Mobile Communication FM or PM Receivers, 25-866MHz."

The receiver shall have intermodulation products no greater than 39 dB via the measurement procedure described in EIA document EIA/TIA-204-D "Minimum Standards for Land Mobile Communication FM or PM Receivers, 25-866MHz."

The information below specifies requirements for the access point and the peripheral transmitters.

The transmitted power in the 1 MHz band defined by the desired channel shall be less than 100 mW (+20 dBm) peak-average. Peak-average is defined as the average power radiated during active transmission and therefore does not change with duty cycle. Note that regulations in some countries limit transmitted power to less than 100 mW. In these countries the more stringent regulations must be adhered to.

The RMS error vector magnitude (EVM) of both the access point and the peripheral shall be less than 12.5% where the RMS EVM is defined as:

$$EVM = 100 * \sqrt{\sum |Sae^{j\theta} - \alpha Si|^2 \Big/ \sum |(\alpha Si)|^2}$$

where Sa is the complex baseband equivalent of the actual transmit signal, Si is the ideal complex baseband equivalent signal, and a and q are constants chosen to minimize EVM. During this measurement the transmitter under test should be locked to the reference signal such that no frequency offset exists in the transmitted signal relative to the reference signal.

Less than 1% of the total transmit power shall occur outside of the desired channel. Total power in any channel 2 MHz or more removed from the center frequency of the desired channel shall be less than 2 mW and the total power in the adjacent channel shall be less than 300 mW during active transmit. Emissions outside of the desired band must meet regulatory requirements for the country of operation.

The spurious output shall be less than -50 dBc. The spurious output shall be determined using a spectrum analyzer with the IF bandwidth set to 100 kHz. The spurious signal shall be measured with the transmitter modulated with random data. The spurious signal level is defined as any spectral component of the modulated signal in a 100 kHz bandwidth offset by more than 4 MHz from the carrier and referenced to the unmodulated carrier power.

Because the access point must transmit to many peripheral devices which are not co-located, dynamic power control on the downlink is not allowed. Power control may

optionally be employed in the peripherals. It is recommended that any peripheral power control algorithm, if used, should target packet error rates below 0.1% to avoid excessive use of system resources due to a large number of retransmissions.

When the access point or peripheral is not in active transmit or the ramp-up or ramp-down condition, the output power in any channel shall be less than 400 nW.

The transmitter shall ramp-up and ramp-down in response to the start or end of a burst in less than 5 symbol periods (6.47 mS) . This period is defined as the duration between the peak of the transmitted impulse due to the first/last symbol of the burst and the point at which the transmit power remains below 400 nW.

The information below gives requirements which apply to reference frequency sources in both the access point and the peripheral.

The access point and the peripheral shall transmit a modulated carrier which is within 25 kHz of the channel centers defined in "Frequency Plan." This is equivalent to 10 PPM accuracy in the source from which the carrier is derived. Symbol timing shall also be accurate to within 10 PPM .

The phase noise measured at the output antenna shall be less than -94 dBc/Hz at a 100 kHz offset from the center frequency.

The channel switching duration between any two channels shall be less than 662 mSec for the carrier frequency to settle to and remain within 12 kHz (5 PPM at a carrier frequency of 2450 MHz) of the final value.

The access point and peripheral must be able to switch between active transmit/receive to receive/transmit in less than 32.383 mS (25 symbols). This switching time is defined as the time from the peak of the impulse due to the last symbol of the transmitted/received burst to the peak of the impulse due to the first symbol of the received/transmitted burst.

The DA-TDMA system assigns each block on an individual basis and allows all blocks to be immediately acknowledged. Assignments are based on connections to applications where each connection corresponds to a unique physical layer address. Within these connections, acknowledgments are used to mitigate the interference caused by microwave ovens and other impediments. The individual blocks may be combined to form isochronous data streams from 1 to 992 kbps or asynchronous data packet up to 6141 octets long. Individual connections can be aggregated to form a full-duplex communications link which may be asymmetrical. A control connection is used to manage the origination and termination of both types of transfers. The control connection is used to manage system parameters such as hopping patterns, devices IDs, etc.

This information defines the requirements of the datalink layer. The Medium Access Layer specifies the addressing formats used to dynamically allocated each block, the control connection extended header, and the random access procedure. The ARQ protocol and scheduling specify the fundamental state machines performed by the access point and peripherals. The Connections describe the types of connections between peripherals and applications, both asynchronous and isochronous. The Messaging procedure for signaling the contents of all the messages for both the datalink and network layer.

Each block is assigned based on source and destination address transmitted in the BA burst. By different pairings of the source and receiver, a uplink, downlink, or pier-to-pier transfer will take place. Addresses are associated with connections to applications and applications determine the destination of transfers. The applications may subsequently direct the DMF function to route the data to another peripheral, forward the data to the wired network, or process the data internally. In any case, a peripheral does not directly address another peripheral.

Special contention blocks provide access to the system for asynchronous traffic using a form of reservation ALOHA. The peripheral will send up a block specifying the length of the transfer and the address of the connection. Contention blocks are always used for the initial access to the system.

Subsequent accesses may take place on the contention block or alternatively the system may require the device be polled periodically on it's control connection. Congestion is avoided by vary the number of devices operating in contention mode, the periods of the polled devices, and the persistence of the contending devices.

Isochronous traffic must negotiate the origination and termination of each connection using asynchronous packets on the control connection. At origination, the peripheral may request the connection or the application may direct the DMF by specifying the number of connections, the respective data rate, and direction of each connection.

The following information defines the fundamentals of the medium access layer. The Addressing portion defines the addressing schemes and the reserved addresses. The Control Connection Extended Header portion defines format of the control connection extended header used for both polled and contention access. The Contention Access portion defines the operation of the contention mode.

Connections between peripherals are uniquely addressed at the medium access layer. Each peripheral is assigned a fundamental and sub-address space at registration as described herein. Several addresses have been reserved by

system and have special meaning. The reserved addresses are as identified herein.

The 12-bit address assigned to each peripheral is broken in to a fundamental address and variable sub-address. The fundamental address identifies the peripheral device while the sub-address identifies a specific connection to an application. The size of the sub-address field will vary per device depending on the number of connections a device is capable of supporting simultaneously. The sub-address may be 0 through 5 bits long and occupy the most significant bits of the address. The fundamental address occupies the remaining 12 to 7 bits of the address.

The fundamental address space is unique over both the source and destination fields while the sub-address may be used to identify two connections, one sourced by the peripheral and the other destined for the peripheral. The fundamental portion of a device's address is the same value in both the source and destination fields. Sub-addresses may be repeated but are always treated as independent connections and maintain individual SBSN.. For example, a full-duplex communication link would use the same numerical sub-address for the both transmit and receive connection to an application. Sub-address zero is always assigned to the default full-duplex control connection with the DMF. A device with a 12-bit

fundamental address may only support the default control connection.

Addresses are reserved to identify the access point as a source or destination, mark a block for contention access, or provide generic address for new devices. Table 8 Reserved Addresses specifies the addresses reserved by the system and identify their purpose.

Table 8 Reserved Addresses

Address (Binary)	Purpose
%00000000000	The "null" address indicates that the source or destination device is the access point.
%1111111XXXX X	Reserved for contention access. The 5 sub-addresses associated with this address specify the various persistence modes and priority levels.
%1010101XXXX X	Reserved for pre-registration. The sub-address field will be selected at random by the registering peripheral providing 32 independent pre-registration addresses.

The control connection defines a special control connection extended header to allow the origination of an asynchronous transfer. All contention accesses, polls, and pages are

assumed to be on the control connection and use the extended header. Likewise, every control connection block must use the extended header. In a contention access or poll, the extended header may request a asynchronous transfer. In a page, the extended may announce an asynchronous transfer.

Table 9, Control Connection Extended Header, defines the fields within the extended header. The Multiple Block bit identifies that an asynchronous transfer is requested to the application specified by the Source Address field. The length of the transfer is specified by the fields, Remaining Blocks, Pad Bits, and Pad Octets. A PPP bit identifies that true destination is specified by the network address enclosed within the data field. A Reservation Sequence Number is used to distinguish between repeated reservation requests.

Table 9 Control Connection Extended Header

Extended Header Fields	Description	Bit Indices (begin/end)		Length
Multiple Block	Indicates that this is a single block transmission and does not require any additional blocks to complete the transmission. A value of 0 indicates a single block.	50	50	1 bit
PPP	Indicates that the true destination is enclosed within the encapsulated Point-to-Point Protocol Packet	51	51	1 bit
Reservation Sequence Number	Used to distinguish between retried reservation requests from a single device	52	52	1 bit
Reserved	Reserved. Encoded as 1	53	53	1 bit
Source Address	Source address to used for subsequent blocks of asynchronous packet. The source address uniquely identifies the corresponding service and format of the enclosed data.	54	65	12 bits

Remaining Blocks	Number of remaining blocks. A value of N implies a packet length of (93+96•N) octets. May take on the value 0 through 63. A maximum of packet length of 6141 octets The single block bit must be set for one block packets.	66	71	6 bits
Pad Bits	Specifies the number of padding bits in the final octet. (The final octet precedes the first pad octet) May take on the values 0 through 7.	72	74	3 bits
Pad Octets	Specifies the number of padding octets in the final block. May take on the values 0 through 95.	75	81	7 bits
Data	Format of the data is determined by the Source Address above.	82	817	93 octets

Contention Access

Peripherals may randomly access the system on specially marked contention blocks. The access point marks a contention block by placing one of the reserved contention addresses in the source address field of a BA burst. Peripherals with data to send then access the system using a dynamic p-persistent CSMA-like protocol. The persistence level may vary at the discretion of the access point depending on the level of congestion and take on the values 1, 1/2 1/4, 1/8 1/16, 1/32,

1/64,or 1/128. In addition, the connection access may be restricted to registration traffic only. The 5-bit sub-address field is used to dynamically specify persistence level and restrictions on the current connection slot. Table 10 defines the format of the contention address.

Table 10 Contention Address Format

Fields	Description	Length
Fundamental Address	Fundamental portion of the contention address. Must be encoded as binary %1010101.	7 bits
Restricted Status	A value of 1 indicates that only registering terminals may access this connection block.	1 bit
Reserved	Must be encoded as 0.	1 bits
Persistence Level	Species the persistence level used by the peripheral in the current block. Value ⇒ Level %000 ⇒ 1 %001 ⇒ 1/2 %010 ⇒ 1/4 %011 ⇒ 1/8 %100 ⇒ 1/16 %101 ⇒ 1/32 %110 ⇒ 1/64 %111 ⇒ 1/128	3 bits

Contention access can be modeled as a slotted aloha system with carrier sensing. The unallocated blocks, remaining after isochronous connections have been serviced, form the slotted aloha channel. An idle system will transmit nothing but connection blocks. A peripheral winning contention would be given the unallocated blocks for the duration of it's transfer. The others peripherals would sense the winning peripheral's activity by the absence of a contention block. Upon completing the transfer, the system will again assign the unused blocks for contention access. The access point controls the back-off of the peripherals in the system. A high persistence value implies a long back-off and low persistence value implies a short back-off.

A peripheral contending on the system will monitor the BA bursts until a c transmission will resume monitoring the BA until it has transmitted. A peripheral will assume it's successful when the source address encapsulated within the extended header is present in the destination field of the next contention slot or a block has been assigned to that address. Either event requires the peripheral to stop contending for TP201.

The information below describes an asynchronous transfers in detail.

The DA-TDMA system integrates a simple stop-n-wait ARQ mechanism with the scheduling algorithm. The ARQ and scheduling work together to transfer N ordered data blocks

from the source device to the destination device. Each transfer is performed by three entities, the scheduler, the source device, and destination device. The scheduler is a sub-function of the DMF running on the access point. It assigns the appropriate number of blocks to support the data transfer and requisite retries. The scheduling function has two levels of responsibility, the multiplexing of the all connections and specific management of individual connections. The ARQ impacts the connection-specific scheduling. The connection-specific scheduler must maintain a accurate count of the successfully transferred blocks, allowing the connection multiplexer to determine when a particular connection's requirements have been met or whether more blocks are required to complete the transfer. The protocol must ensure that the source's, destination's, and scheduler's counters remain synchronized.

The ARQ protocol performs the following steps for each data block transferred:

1. The access point transmits the block assignment burst specifying the source and destination device in the address fields. The source and destination devices may be both peripherals forming a coordinated pier-to-pier transfer. Alternatively, either the source or destination device may be the access point forming a downlink or uplink transfer, respectively.

2. The source device then sends the payload burst to the destination device including a 1-bit Block Sequence Number. One sequence number is maintained per each sub-address on a device. The sequence number is set to zero at the beginning of each transfer.

3. Having received the payload burst the destination device sends a ACKSEQ burst to the access point. The ACKSEQ burst positively or negatively acknowledges the reception of the payload burst. If positively acknowledged, the ACKSEQ burst also forwards the value of the sequence number. The access point is not required to receive the payload burst in pier-to-pier transfers.

4. Upon receiving the ACKSEQ, the access point echoes the acknowledgment, less the sequence number, in the next block assignment burst.

5. The source peripheral receives the acknowledgment and determines whether it must retry the previous block. The acknowledgment is always received prior to transmitting the next payload burst.

The informaiton below specifies the operation of the source device, destination device, and connection-specific scheduler with respect to the ARQ algorithm. It exactly specifies when the Block Sequence Number and transfer count are incremented by all three communicating entities insuring that all blocks get communicated in order and that all three entities complete the transfer simultaneously.

A source device must follow the flow diagram illustrated in FIG. 18, 1800. After negotiating the length of the transfer and the address of the connection, source device initializes it BSN and block count to zero (1802) and then begins waiting for assigned blocks. Upon receiving a BA burst containing its source address (1804), the source device transfers a payload burst (1806) to the destination device. Completing the transmission, the source device receives the acknowledgment in the BA burst of the next block. The source device does not decode the ACKSEQ burst. If the block was negatively acknowledged, the source device continues waiting for assigned blocks and will retransmit the current block when the next assigned block arrives. If the block was positively acknowledged (1808), the source device increments (1810) the block sequence number and the count of blocks transferred (1812). If there are no more blocks in the sequence, the source device exits (1816) the transfer mode. Otherwise the source device gets the next block in the sequence and continues waiting for assigned blocks.

A destination device must follow the flow diagram illustrated FIG. 19, numeral 1900. After negotiating the length of the transfer and the address of the connection, the device initializes its expected BSN and block count to zero (1902) and then begins waiting for assigned blocks. (1904) Upon receiving a BA burst (1906) containing its destination address, the device receives a payload burst from the source device. If payload burst was received in error (1907), the device

transmits an ACKSEQ burst representing a NAK (1922) to the access point and then resumes waiting for assigned blocks. If the payload burst was received successfully, the device transmits an ACKSEQ representing an ACK-0 or ACK-1 (1908) depending on the BSN of the payload burst. It then checks the received BSN against the expected BSN (1910). If they match, the device accepts the data block (1912), increments it expected BSN (1914), and increments its count of transferred blocks (1916). If all the blocks have been received (1917), the device exits the transfer mode (1918). Otherwise, the device continues waiting (1920) for block assignments. If the received BSN does not match the expected BSN, the block is discarded (1924).

The connection-specific scheduler must follow the flow diagram illustrated in FIG. 20, numeral 2000. After negotiating the length of the transfer and the address of the connection, the connection specific scheduler initializes its expected BSN and block count to zero (2002) and then begins waiting for assigned blocks (2004). Upon detecting a BA burst containing the source/destination pair, the access point receives an ACKSEQ burst from the destination device (2006). If the ACKSEQ burst represents a NAK (2007), the connection-specific scheduler forwards a NAK (2008) to the source device in next BA burst and resumes waiting for assigned blocks. If the ACKSEQ burst represents a ACK-0 or ACK-1, the scheduler forwards an ACK to source device (2010)in the next BA burst and then compares the ACK-value against the expected

sequence number (2012). If the sequence number and ACK-value match, the connection-specific scheduler increments it expected BSN (2014), and increments its count of transferred blocks (2016). If all the blocks have been transferred (2018), the scheduler exits the transfer mode and instructs the multiplexing scheduler to stop assigning blocks to the connection. Otherwise, the scheduler continues waiting assigned blocks.

The system support two types of connections, asynchronous and isochronous. Asynchronous connections allow for the transfer of data bursts at up to 1 Mbps. Isochronous connections support the periodic transmission of delay sensitive natural traffic types. Both connections employ the ARQ algorithm defined in the previous section. The following sections define the two connection types and their governing protocol timers and counters.

An asynchronous connection transfer an aperiodic data packet between a peripheral device and application. The most common data type transferred are PPP encapsulated IP datagrams. Each asynchronous connection is established during the registration process and is maintained for the duration a device is registered.

The data packet is segmented by the source device into native payload blocks called asynchronous segments. The first segment is a control segment followed by the requisite number of data segment. Ninety-two octets of a data packet may be

included in the control segment. Each subsequent data segment may carry 96 octets of the data. The final data segment will be padded will fill bits to form one complete block. The end of the data in the final segment is specified in the initial control segment's Pad-Octets and Pad-Bits fields. See the information on Control Connection Extended Header for the format of the initial control segment.

FIG. 21, numeral 2100, illustrates a peripheral originated transfer on the PPP asynchronous connection. A peripheral-originated asynchronous transfer begins by the peripheral device (2102) transmitting the control segment on either a marked contention block or in its assigned polling block. The initial control segment specifies the length of the transfer in blocks and the asynchronous connection address. The access point (2104) responds by initializing a connection-specific scheduler to transfer the requested number of blocks from the source address specified and then assigns blocks until the transfer is complete. The source peripheral participates in the transfer performing the ARQ/scheduling algorithm defined in the ARQ protocol and scheduling information .

FIG. 22, numeral 2200, illustrates a peripheral terminated transfer on the PPP asynchronous connection. A peripheral-terminated asynchronous transfer begins with the access point (2204) announcing the transfer by transmitting the control segment during the peripheral's paging interval. Like a

peripheral originated transfer, the initial control segment specifies the length of the transfer in blocks and the asynchronous connection address. The peripheral (2202) responds by suspending it's current standby mode and listening for blocks containing the asynchronous address in the destination field. The peripheral and access point then perform ARQ/scheduling algorithm defined with respect to ARQ protocol and scheduling.

Asynchronous connections, like all connections, are between peripherals and applications. However, the data contained within an asynchronous transfer may be destined for another peripheral. For example, the IP address with an PPP encapsulated IP datagram may specify another peripheral. In this type of transfer, the application may simply store the entire asynchronous packet received from the source peripheral and then forward the packet to the destination peripheral in a subsequent asynchronous transfer. Alternatively, the application may direct the DMF to set-up a pier-to-pier connection between the peripherals. FIG. 23, numeral 2300, illustrates a pier-to-pier asynchronous transfer. Like a peripheral originated transfer, the source peripheral (2302) sends the control segment to the access point (2306). The application within the access point identifying the destination peripheral (2304) as another peripheral would direct the DMF to announce the transfer to the destination peripheral. The 92-octets of data contained in the source's control segment would be transferred to the

destination in the announcement. All subsequent data segments would be transferred directly between the source and destination peripheral. From the peripheral's prospective, a pier-to-pier transfer is indistinguishable from access point terminated/origination connection.

Several protocol timers regulate the asynchronous transfer process. TP202 specifies the maximum time between the transmission of the initial control segment and when the first block is assigned for a data segment. TP203 specifies the maximum time between assigned blocks for data segments. NP201 specifies the maximum number of retries on any particular block in the sequence. If any of these protocol parameters are exceeded the peripheral must abort the transfer and either retry or drop the packet.

Isochronous connections provide means for transmitting delay sensitive data such as natural traffic types or particularly voice samples. Like asynchronous traffic, the ARQ/scheduling mechanism transports the voice samples making them robust to interference. Low-delay is achieved by bounding the period in which a particular set of samples may be retried. This retry period is referred to as an Isochronous Window (IW) and is equal in duration to one DA-TDMA frame. An IW, however, may be assigned various frame offsets unique to the connection. For example, an IW beginning on block 5 in one frame would end on block 4 of the next frame. A series of IWs chained together form an isochronous connection. Within

each IW, the ARQ/scheduling algorithm is performed to transfer a fixed number of blocks. The number of blocks, the frequency of the IWs, and the direction of the transfer are negotiated during an isochronous set-up.

A peripheral in the isochronous mode may support multiple number of isochronous connections differentiated by unique sub-addresses. Each isochronous connection will specify a fixed number blocks to transfer per IW and the direction of the transfer. The number of blocks determines the data rate for the transfer with one block per IW forming the fundamental data rate 32 kbps. Super-rate and sub-rate connections are also possible. A super-rate connection is formed by transferring multiple blocks per IW giving a Nx32 kbps data-rate. Sub-rates are formed by transferring one block every M IWs giving a 32/M kbps data-rate. In the typical case of a POTS application, the peripheral will support two isochronous connections, one for the uplink and the other downlink, each assigned one block per IW. Therefore, the POTS peripheral would make two transfers every IW. In general, a combination of sub-rate, super-rate, and fundamental-rate traffic may have the peripheral transferring a varying number of blocks from one IW to the next. The number of blocks transferred during particular IW is always deterministic.

A peripheral may discontinue reception during periods of inactivity to conserve power. After receiving the expected number of blocks for an IW, a peripheral may be assured that access point will not assign blocks to it until the beginning of the next IW. At that point, it may power down it's receiver balance of the current IW. Therefore, a scheduler with out-of-band control signaling must send it's information prior to the isochronous blocks scheduled for the IW. On sub-rate connections, a peripheral may also discontinue reception between IW intervals. In the event of errors in the block transfer, the peripheral must continue to receive until all scheduled blocks retried successfully.

Isochronous transfers are initiated through a negotiation on the peripheral's control connection. FIG. 24, numeral 2400, illustrates an isochronous origination and termination. The peripheral (2402) may initiate the process by transmitting an asynchronous Isochronous Set-up on a contention block containing uplink/downlink data-rates and application requested. The access point(2404) sends Isochronous Assignment containing isochronous address(es) for connection, starting frame and frame offset. Optionally, services may be denied with an Isochronous Reject. Isochronous communications ensues. Supplemental control information may be exchanged asynchronously during the connection. A peripheral with control data pending sets the Control Connection Status bit in the payload header indicating that a

control information is pending. Detecting the control connection status, the access point should assign a block to the peripheral's control connection in the next IW. An access point with control data simply sends the information prior to the isochronous blocks. The connection may be terminated by either the peripheral or access point. When terminated by the peripheral, the peripheral sends an asynchronous disconnect request to the access point. The access point responds with a disconnect order. When terminated by the access point, the access point simply sends an unsolicited disconnect order.

The access point is responsible for managing the systems resources and must enforce an admittance policy reserving bandwidth for retransmission's. When the capacity is exceeded, isochronous connections will be denied. The system's isochronous capacity is shared.

Two timer govern the isochronous connection, TP204 and TP205. TP204 defines the retry period for isochronous set-up messages. If the access point does respond to an isochronous set-up within TP204, the peripheral may resend the set-up message. TP205 defines the maximum interval between successful IW transfers. A peripheral will restart TP205 when it has received all the scheduled isochronous blocks within one IW. Therefore, one successful IW transfer every TP201 is enough to keep a connection active. Should TP205 expire, the peripheral will attempt to return to it's standby mode. The

access point maintains a equivalent timer to TP205, TA205, and will also drop the connection.

A peripheral registered with a system will, in general, spend the most time in a standby mode. The standby mode allows the peripheral to conserve its power while not actively engaged in a isochronous or asynchronous transfer. Two types of standby modes are supported, a Discontinuous Reception (DRX) or Polled mode. These modes are similar to isochronous sub-rate connections expect the period between IWs may be much longer, from seconds to minutes. The DRX mode is like a downlink isochronous connection and the polled mode is like a uplink isochronous connection. A peripheral in the DRX mode uses contention slots to transmit uplink control information while a polled peripheral must wait until it is polling interval. Peripherals in either mode may receive messages, referred to as pages, during their scheduled IWs, referred to as both paging or polling intervals. All uplink and downlink messages during standby mode are addressed to the control connection. The DRX mode is intended to complement the asynchronous protocol by supporting units with varying data loads and low delay requirements. The polled mode may be used to alleviate congestion by relegating all delay insensitive devices to infrequent polling. The polled mode may also be selected if the maximum delay must be bounded since a peripheral will have an opportunity to access the system every polling interval. The access point determines whether a peripheral is assigned to a

DRX or polled mode in order to balance the system's performance for all peripherals. Each peripheral must support both DRX and polled modes for all applications.

In general any type of data may be sent in the paging/polling interval. In the simplest form it may be used to transmit a single control message or possibly a very low-speed isochronous data stream. Alternatively, the paging message may direct the unit to suspend the standby mode. In this case, the paging message would contain an isochronous announcement or be the initial segment in a multi-segment asynchronous transfer. Likewise, a peripheral may suspend the standby mode by transmitting similar messages on the uplink. Upon termination of the isochronous connection or completion of the asynchronous transfer a peripheral would return to the standby mode. Optionally, a peripheral may delay the return to standby to allow for consecutive asynchronous transfers.

The DRX can be thought of as a special kind of isochronous transfer which is unidirectional, from the access point to the peripheral, and carries an assignment of zero bursts per period. The period is called a paging interval. Each unit is assigned a duration between paging intervals and frame offset at which the paging interval starts. The unit must correctly receive one burst per paging interval. Afterwards, the unit may discontinue reception until the next interval and conserve power. Note, the burst received does not have to be addressed

to the unit to satisfy the protocol. In this way, several units may be multiplexed onto the same paging period.

In DRX mode, the peripheral is assigned a set paging interval reoccurring every N frames at a predefined frame offset starting at block M. The peripheral is required to begin monitoring the block assignment field starting at frame N, block M, until it correctly demodulates a block assignment.

During an inactive paging interval, the access point may send data to other peripherals at its discretion. The peripheral will demodulate one block assignment, determine the message is for another user and return to low-power mode until the next paging interval.

During an active paging interval, the access point must repeat the message in consecutive blocks until properly acknowledged. The access point is assured the peripheral will continue to listen until the microwave oven inference subsides.

A peripheral with data-to-send may contend on any available contention block.

Two counters govern the DRX mode, NP202 and NA204. NP202 defines the maximum number of consecutive erroneous BA bursts a peripheral may receive. If NP202 is exceeded the peripheral must attempt resynchronize to the system. NA204

defines the maximum number of consecutive paging intervals in which a peripheral does not acknowledge a page that an access point must tolerate. If NA204 is exceeded, the peripheral is de-registered by the access point.

A peripheral in DRX mode must periodically re-register with the access point to insure that it has not been inadvertently de-registered. The re-registration period is assigned as part of the standby mode information element defined in section 3.3.5.5.15. Section 3.4.3 Re-registering peripherals defines the re-registration process.

Polled Mode

The polled mode is essentially a sub-rate isochronous transfer which is unidirectional, from the peripheral to the access point, and carries an assignment of one burst per period. The period is called a polling interval. Each unit is assigned a duration between polling intervals and frame offset at which the polling interval begins. The unit must successfully transmit one burst per polling interval. If the peripheral has no data to transmit, it will send a Null control message. Afterwards, the unit may discontinue reception until the next polling interval and conserve power.

In the polled mode, the peripheral is assigned a polling interval reoccurring every N frames at predefined frame offset starting at block M. The peripheral is required to begin monitoring the block assignment field starting at frame N, block M until it transmits a uplink block or one frame-period expires.

During an inactive polling interval, the access point should assign an uplink block to the peripheral before one frame-period expires.

During an active polling interval, the access point must transmit the downlink message to the peripheral prior to assigning an uplink block.

A peripheral with data-to-send must wait until the next polling interval

Two counters govern the polled mode, NP203 and NA203. NP203 defines maximum number of consecutive polling intervals in which a peripheral does not receive an uplink block assigned to it's uplink control connection. If NP203 is exceeded the peripheral must attempt re-reregister with the system. NA203 defines the maximum number of consecutive polling intervals in which a peripheral does not respond to an uplink block assignment. If NA203 is exceeded, the peripheral is de-registered by the access point.

Messaging

The peripheral communicates with the DMF in the access point over the control connection. The control connection is always addressed to the fundamental address and sub-address zero on both the uplink and downlink, see section 3.3.1.1. An uplink control message may be sent on any available contention block, polled block or other directly address control block while a downlink control message may be sent during a page or some other period the peripheral is known to be listening.

All control messages use the Control Connection Extended Header, described in section 3.3.1.2, along with a Control Message Header, described in section 3.3.5.1. All control messages are asynchronous in nature and are transmitted using an asynchronous transfer.

In support of the variety of peripherals operating on the In-Home RF Bus and realizing that some may not be as capable as others, a concept of control message pacing is provided on the control connection. Peripherals capable of streaming control messages at the 1 Mbps maximum system transfer rate may use a direct asynchronous transfer to transmit the longer multi-block control messages. These control messages would be scheduled as a multi-segment asynchronous transfer. Peripherals with less processing capabilities may select to have their control messages paced. In the latter case, these peripherals will divide a long control messages into multiple single-segment asynchronous transfers each carrying one block of the multi-block control message. The multiple single segments may be reconstructed by using sequence information contained in the control message header.

The following sections define the control messages used by the In-Home RF Bus. Section 3.3.5.1 defines the format of the control message header. Section 3.3.5.2 discusses the operation of control message pacing. Section 3.3.5.3 lists all the control messages and their corresponding code-points. Section 3.3.5.4 provides detailed information on each control message including the required and optional information

elements. Finally, section 3.3.5.5 defines the coding of each individual information element.

Control Message Header

Control messages are carried within the 96-octet data field of the payload burst. Every block within a control message will use the 32-bit Control Connection Extended Header reducing the available octets in the data field to 92. The coding of these remaining octets are defined below:

Octet field	Description	Length
Protocol Version	Marks the revision of the In-Home RF Bus control message protocol. Version 0 is defined by this document.	1 octet
Message Type	Identifies the control message which defines the purpose as well as the required and optional information elements contained. The available message types and their corresponding code-points are defined in section 3.3.5.3.	1 octet
Message Length	Length of the control message in blocks. This field may take on the value 1 to 255. The value in this field is repeated in every block of a multi-block control message.	1 octet
Message Block	Index of the current message block. This field may take on the values 1 through 255. The first block in a multi-block control message is numbered 1.	1 octet

Information Elements	Information elements are defined by the message type above. Messages may specify both mandatory and optional elements. Section 3.3.5.4 Control Message Formats defines the mandatory and optional elements per message.	88 octets

TABLE 11

The control connection provides a method to pace control messages to match the capability of the particular peripheral in terms of buffering and processing. Three paces are provided full-rate, medium-rate and low-rate. At the full-rate, the control connection may deliver every block of a multi-block control message in successive blocks on the physical interface. At the medium-rate, blocks are delivered to the control connection no faster then every fourth block on the physical interface. At the low-rate, only one block may be delivered per frame and no faster then one block every thirty-second block on the physical interface.

Full-rate peripherals may use the asynchronous transfer mechanism to transport multi-block control messages. The first block in the message would identify the message as a multi-segment transfer in the Control Connection Extended Header allowing the DMF to schedule the transfer at the medium access layer. All remaining blocks would be identified as single segment transfers in the Control Connection Extended

Header allowing the blocks to pass through the medium access layer. For consistency with medium-rate and low-rate peripherals, the Control Message Header would also contain sequence information. The sequence information is redundant since the medium access layer would have delivered the multi-block message in-order to the DMF.

Medium-rate and low-rate peripherals would bypass the asynchronous transfer mechanism when transporting multi-block control messages. All blocks would be identified as single segment transfers and be passed through the medium access layer. Sequence information within the Control Message Header would be used to reconstruct the message by the DMF.

Table 12 below specifies the value, direction and reference for each message used by the datalink and network layers. The direction is defined as uplink, downlink or bi-directional. Uplink messages are always sent by the peripheral to the access point. Downlink messages are always sent by the access point to the peripheral. Finally, bi-directional messages may be sent by either the peripheral or access point.

Value	Message	Direction	Reference
0	Registration Request	Uplink	3.3.5.4.1
1	Registration Assignment	Downlink	0
2	Registration Reject	Uplink	3.3.5.4.3
3	Authenticity Challenge	Bi-directional	0
4	Authenticity Response	Bi-directional	3.3.5.4.5
5	Service Set-up	Uplink	3.3.5.4.6
6	Service Assignment	Downlink	3.3.5.4.7
7	Service Negotiation Complete	Uplink	0
8	Isochronous Set-up	Uplink	3.3.5.4.9
9	Isochronous Assignment/Announcement	Downlink	0

10	Isochronous Reject	Downlink	0
11	Disconnect Request	Uplink	0
12	Disconnect Order	Downlink	0
14	Application Information	Bi-directional	3.3.5.4.14
15	Null	Bi-directional	3.3.5.4.15

TABLE 12

This section defines the information elements contained within each control message. It is assumed that mandatory elements must appear at the beginning of message and order is important. Furthermore, all mandatory elements have a fixed length. Optional elements appear after the mandatory elements and must be identified by an information element identifier followed by length field in octets. Order is also important for optional elements. Although, optional element may vary in length.

Registration Request

The registration request is sent by the peripheral to the access point to initiate access to the system.

Information Element	Reference	Type	Length
Random		M	4
Number of Connections		M	1
PIN		M	12
Control Segment Pace		M	1
Language Identifier		M	1
Fill Pattern		M	69

TABLE 13

Registration Assignment

The registration response is sent by the access point as a affirmative response to a registration request. The message registers the peripheral with the system.

Information Element	Reference	Type	Length
Random		M	4
Fundamental Address		M	2
Scramble Code Index		M	2
Frequency Hopping Pattern		M	80
System Specific ID		O	14
Peripheral ID		O	6
Control Channel Access		O	1
Fill Pattern		M	81

TABLE 14

The registration reject is sent by the access point as a negative response to a registration request.

Information Element	Reference	Type	Length
Random		M	4
Cause		M	4
Language Identifier		M	1
Fill Pattern		M	79

TABLE 15

The authenticity challenge is sent by the access point or peripheral challenging the authenticity of the other device.

Information Element	Reference	Type	Length
Random Challenge		M	8
Fill Pattern		M	80

TABLE 16

The authenticity response is sent by the access point or peripheral challenging in response to an authenticity challenge.

Information Element	Reference	Type	Length
Random Challenge		M	8
Challenge Response		M	8
Fill Pattern		M	72

TABLE 17

The service set-up is sent to the peripheral as part of the registration process. It contains preferred default settings for a one or multiple applications.

Information Element	Reference	Type	Length
Applications Initialization Request (multiple instances)		O	*

TABLE 18

The service assignment is sent by the access point to the peripheral specify the assigned application settings. The settings are negotiable and the peripheral may respond with alternative settings in subsequent service set-up.

Information Element	Reference	Type	Length
Standby Mode		M	9
System Specific ID		M	12
Peripheral ID		M	4
Application Assignment (multiple instances)		O	*

TABLE 19

The peripheral sends a service negotiation complete indicating the accepted applications and completing the service negotiation.

Information Element	Reference	Type	Length
System Specific ID		M	12
Peripheral ID		M	4
Application Identifier (Multiple)		O	3
Fill Pattern		M	*

TABLE 20

The isochronous set-up is sent by a peripheral to request a isochronous connection be established between it and the specified application.

Information Element	Reference	Type	Length
Application Identifier		M	1
Isochronous Connection Request		M	1
Isochronous Connection Request (Multiple)		O	3
Application Information		O	*
Fill Pattern		M	*

TABLE 21

The isochronous assignment/announcement is sent by the access point establishing one or multiple isochronous connection.

Information Element	Reference	Type	Length
Application Identifier		M	1
Frame		M	3
Frame Offset		M	1
Connection		M	2
Connection (Multiple)		M	4
Application Information		O	*
Fill Pattern		M	*

TABLE 22

The isochronous reject is sent by the access point in response to a isochronous set-up. The message may deny services when isochronous resources are not available.

Information Element	Reference	Type	Length
Application Identifier		M	1
Isochronous Connection Request		M	1
Isochronous Connection Request (Multiple)		O	3
Fill Pattern		M	*

TABLE 23

The disconnect request is sent by the peripheral to request that an isochronous connection be discontinued.

Information Element	Reference	Type	Length
Application Identifier		M	1
Connection		M	2
Connection (multiple)		O	4
Application Information		O	*
Fill Pattern		M	*

TABLE 24

The access point sends a disconnect order to terminate one or multiple existing isochronous connection. The message may be sent unsolicited or in response to a disconnect request.

Information Element	Reference	Type	Length
Application Identifier		M	1
Isochronous Frame		M	2
Connection		M	2
Connection (multiple)		O	4
Application Information		O	*
Fill Pattern		M	*

TABLE 25

Application Information message carries data between applications and their clients. The message may be sent by the access point or peripheral.

Information Element	Reference	Type	Length
Application Identifier		M	1
Application Information		O	*
Fill Pattern		M	*

TABLE 26

The message is usually sent during a polling interval when the peripheral has no control data to send. In general, it may be sent by either the access point or peripheral.

Information Element	Reference	Type	Length
System Specific ID		M	12
Peripheral ID		M	4
Fill Pattern		M	73

TABLE 27

This section defines the format and content of the information elements sent in the messages defined in section 3.3.5.4. The information elements may preceded by an information element identifier and length field. When the information element is mandatory and fixed length, it is not preceded by an information element identifier and length field. When information is optional or variable length it must always be preceded by an information identifier. The following table28 defines the value of the information element identifiers.

Value	Message	Direction	Reference
0	Random		3.3.5.5.1
1	Number of Connections		3.3.5.5.2
2	PIN		3.3.5.5.3
3	Control Segment Pace		3.3.5.5.4
4	Null Field		3.3.5.5.5
5	Fundamental Address		3.3.5.5.6
6	System ID		3.3.5.5.7
7	Scramble Code Index		3.3.5.5.8
8	Control Channel Access		3.3.5.5.9
9	Frequency Hopping Pattern		3.3.5.5.10
10	Fill Pattern		3.3.5.5.11
11	System Specific ID		3.3.5.5.12
12	Peripheral ID		3.3.5.5.13
13	Application Initialization Request		3.3.5.5.14

14	Standby Mode		3.3.5.5.15
15	Application Assignment		3.3.5.5.16
16	Application Identifier		3.3.5.5.17
17	Isochronous Connection Request		3.3.5.5.18
18	Application Information		3.3.5.5.19
19	Frame		3.3.5.5.20
20	Frame Offset		3.3.5.5.21
21	Isochronous Connection		3.3.5.5.22
22	Cause		3.3.5.5.23

TABLE 28

A 32-bit random value selected at registration by the peripheral and echoed by the access point.

The number of simultaneous connections the peripheral supports based on application requirements and hardware

capability. The smaller number of the sum of the maximum connections per application or the maximum connections the hardware is capable of supporting.

A Peripheral Identification Number which uniquely identifies the peripheral.

The Control Segment Pace indicates the capabilities of the control interface in the peripheral. It is a measure of the peripheral's processing power and buffer depth.

Value	Interpretation
0	The peripheral supports the full-rate pace.
1	The peripheral supports the medium-rate pace.
2	The peripheral supports the low-rate pace.

TABLE 29

A null field always encoded as zero. May be variable length.

Assigns the fundamental address of the peripheral. The format is defined in the table below.

Table30 Fundamental Address Assignment

Extended Header Fields	Description	Length
Sub-Address Depth	Number of LSBs in the address that represent sub-address space. A value may range from 0 to 5.	3 bit
Reserved	Encoded as one.	1 bit
Address	A 12 bit value between 0 and 4095.	12 bit

System ID: Short ID selected at random to identify the system from among it's neighbors. Broadcast in every BA burst and payload burst.

Scramble Code Index specifies the scrambling code used by the system.

Control Channel Access determines whether the service negotiation is completed on a polled or contention basis. The information element is always optional. When it is not sent, the default is contention access.

Fill Pattern is a special information element used to fill the empty space at the end of block. It does not contain a length field. When encountered by the message parser at the receiver, the parser should skip to the next message block in

the message. A binary value of %00011011 fills the remainder of the block.

System Specific ID is a 12 octet system specific ID. The first 4 octets identify the manufacturer of the device. The remaining octets are required to be unique for every access point manufactured.

Peripheral ID is selected by access point to uniquely identify a peripheral when reregistering. The peripheral will store this value on initial registration. The peripheral can assume previously negotiated services and sub-addresses are still valid if the Fundamental Address, Peripheral ID, and System Specific ID match a set of values cached. Otherwise, services and sub-addresses must be negotiated.

Application Initialization Request is used during service negotiation to initialize an application. The peripheral specifies which application it would like to connect to and identifies it capabilities to the application server. The format of the information element is in Table 31.

Table 31Application Initialization Request Format

Fields	Description	Length
Application Specific Identifier	Uniquely defines the application to connect too.	4 octets
Application Information	As required by the application definition.	0 to 82 octets

Standby Mode assigns the standby mode for the peripheral—either polled or discontinuous reception, the frame offset, and the start frame.

Table 32 Standby Mode Format

Fields	Description	Length
Mode	Sets the standby mode to either polled or discontinuous reception. A value of 1 indicates a poll a value of 0 indicates discontinuous reception.	1 octet
Period	Number of frames between pages or polls. May take on the values 0 through 524287. Allows for a maximum standby of 3.5 hours and a minimum of 24 milliseconds.	3 octets
Frame Offset	Specifies the block in the frame of the paging interval. May take on the values 0 to 30.	1 octets
Start Frame	The frame at which the first paging interval will begin. May take on the values 0 through 524287. Equivalent to the 19 bit frame number in the block assignment burst.	3 octets
Re-registration Period	Specifies the multiple of paging periods after which the peripheral must re-register with the system. A value of 0 indicates that re-registrations are not required.	1 octet

Application Assignment is used during service negotiation to initialize an application. The peripheral specifies which application it would like to connect to and identifies it capabilities to the application server. The format of the information element is in

Table 33 Application Assignment Format

Fields	Description	Length
Application Identifier	Assigns a short 8-bit identifier to the application for further reference. The shorten 8-bit identifier is used for subsequent reference and is unique to a particular access point.	1 octet
Application Specific Identifier	Uniquely defines the application.	4 octets
Application Information	As required by the application definition.	0 to 82 octets

Application Identifier is an 8 bit identifier used as a short-hand for the Application Specific Identifier. It is assigned during service negotiation in the Application Assignment information element. A response to a Service Request. Acknowledging requested parameters or denying service.

Isochronous Connection Request specifies the desired isochronous connection including the direction and the rate.

Table 34 Isochronous Connection Request

Fields	Description	Length
Direction	A value of 0 indicates an uplink connection is required, from peripheral to access point. A value of 1 indicates a downlink connection is required, from access point to peripheral.	1 bit
Mode	A value of 0 indicates a sub-rate connection is requested while a value of 1 denotes a super-rate connection is	1 bit
Reserved	Reserved. Must be encoded as 0.	1 bit
Rate	For sub-rate traffic, the field specifies the number of frames between blocks and may take on the values 1 through 5 providing a 1 to 16 Kbps data-rate. For super-rate traffic, the field specifies the number of blocks per frame and may take on the values 1 through 31 providing a 32 to 992 Kbps data rate.	5 bits

Application Information carries application information.

Table35 Application Information Format

Fields	Description	Length
Application Identifier	Assigns a short 8-bit identifier to the application for further reference. The shorten 8-bit identifier is used for subsequent reference and is unique to a particular access point.	1 octet
Application Information	As required by the application definition.	0 to 82 octets

The frame at which a service change will begin or end. May take on the values 0 through 524287. Equivalent to the 19 bit frame number in the block assignment burst.

Frame Offset specifies the block in the frame where the Isochronous Window begins and may take on the values 0 to 30.

Isochronous connection references an existing isochronous connection or assigns a physical address for a new isochronous connection. Must be a sub-address of the fundamental address. The field is 2 octets long containing a 12-bit physical address.

The Cause indicates the cause with respect to the denial of service or termination.

Table 36 Cause Values

Value	Interpretation
0	"Peripheral has not been registered with this access point."
1	"Bandwidth is unavailable."
Others	Reserved.

The network layer is responsible for maintaining the integrity of the network by keeping track of registered peripherals, available applications, and performance of the air-interface. The access point must manage the peripherals registered with the system. It must be able to identify its own peripherals from those of its neighbor. Furthermore, it must determine whether peripherals are powered-down or out-of-reach. In addition, it must coordinate and convey air-interface parameters such as frequency hopping patterns, scrambling masks, and color codes. Finally, it must be capable of authenticating peripherals and proving its own authenticity to those peripherals.

One system may encompass peripherals made by a variety of manufacturers and purchased independently. In order to associate peripherals with a access point, the access point and peripheral must share a unique Peripheral Identification Number (PIN) and may also share a Peripheral Secret Key (PSK). Every peripheral must be manufactured with a unique PIN.

Peripherals supporting authentication must also contain a PSK. Upon purchasing a new peripheral, both the PIN and PSK must be entered into the access point. The PIN would be transmitted on the A-Interface by the peripheral used to index the PSK at the access point. The PSK would never be transmitted. A variety of methods may be employed to enter the PIN and PSK. For example, many peripherals will provide application software or drivers in support of their device. The PIN and PSK may be included on the distribution media and loaded when the software is loaded. Alternatively, the PIN or PSK may be typed in at a keypad or keyboard which is in some way connected to the access point either to the computer, on a registered peripheral, or as an integral part of the access point.

Often, it is expected that consumers will forgo strong authentication in favor of a simpler configuration process. The PIN is a relatively short 10 character sequence uniquely identifying the peripheral. The PSK is a 50 character secret key in addition to the 10 character PIN. Typing in the PIN/PSK combination may prove too cumbersome to for most consumers. Distributing the PIN/PSK with the application software should make the authentication more assessable, but not all peripheral will come with custom applications. Furthermore, forgoing the authentication enables a simpler peripheral discovery process.

The following sections discus the protocols used to register peripherals with access points. Section 3.4.1

discusses the process of registering new peripherals including the synchronization, authentication, and service negotiation processes. Section 3.4.2 discusses the events which may cause a peripheral to be automatically de-registered from the system. Finally, section 3.4.3 discusses a streamlined process for re-registering known peripherals with the system.

In order for a peripheral to acquire a new system and access service the peripheral must be able to synchronize to an access point, reject access points that are not its own, and finally identify the purchaser's access point as its own. The purchaser's access point and peripheral are assumed to share a PIN which is unique to the new peripheral.. In secure systems, the access point and peripheral are assumed to also share a PSK. The method for inserting the PIN and PSK into the access point is left to the manufacturer's desecration.

FIG. 25, numeral 2500, illustrates one possible state machine a peripheral (2502) might follow when synchronizing to a new system. FIG. 26, numeral 2600, presents the message sequence diagram of the registration process. The peripheral will start by searching for the synchronization pattern on a initial frequency (2602). If no synchronization pattern is detected in TP301, then the peripheral systematically change frequencies and resume searching for the synchronization pattern. If synchronization sequence is detected, the peripheral sends a Registration Request on an available contention access block. Within TA302 (equivalent to TP302),

the access point (2504) must respond with a Registration Assignment or Registration Reject. If the peripheral is rejected the peripheral changes frequency and resumes searching for the synchronization pattern.

When a peripheral is accepted by a access point, the peripheral receives its fundamental address, frequency hopping table and scramble code index from the access point in the Registration Assignment. Also included in the registration assignment is a System Specific ID which uniquely identifies the access point and system assigned Peripheral ID which may be used in subsequent re-registrations to uniquely identify the system and peripheral.

A peripheral will authenticate the network by issuing a Authenticity Challenge message containing a random number that the must be combined with the PSK using an authentication algorithm to produce a challenge response. The challenge response is communicated back to the peripheral in Access Point Response message. The peripheral would compare the challenge response with one generated locally and if they match the access point has been authenticated. Likewise, the access point may initiate authenticate the network using the same Authenticity Challenge and Challenge Response message pair. Note, that is no case is the PSK transmitted over the air interface maintaining it secrecy.

The next step in the registration process is the service negotiation phase. The peripheral initiates the process by sending a Service Set-Up message to the access point. The Service Set-Up message contains one or multiple Application Initialization Request information elements. The Application Initialization Request information contains an Application Specific Identifier which uniquely identifies the application along with requested application setting. Each application initialization request is forwarded to the installed application which interprets the information and generates a response contain application settings in the form of an Application Assignment information element. The DMF appends a shorten one-octet application identifier for future references to the application. If the application identified is available the DMF generates an Application Unavailable information element as a response to the initialization request. All application responses are combined and sent to the peripheral in a Service Assignment message. If the peripheral is dissatisfied with any Application Assignment, it make send up a subsequent Service Set-Up containing alternative application settings. This process will continue until the peripheral receives a set of parameters it is satisfied with or chooses not subscribe to the services of an application. Having reached that point, the peripheral ends the negotiation process by sending a Service Negotiation Complete containing the Application IDs of the application it has chosen to subscribe too. Omitted Application IDs are assumed to have been rejected and

therefore the access point may release any previously negotiated resources associated with the rejected applications.

In the service negotiation process the access point determines an appropriate standby mode with respect to the latency requirements of the applications a peripheral has subscribed too. The standby mode is usually transmitted in the Service Assignment information element but may be reassigned at anytime a peripheral is registered with the system. At the end of the negotiation process, the peripheral enters the low-power standby mode. The peripheral exits the standby mode when it performs an isochronous or asynchronous transfer and returns to the standby mode when the transfers are complete.

During the course of normal operations there are many events that may cause a peripheral to be de-registered by the access point or may make the peripheral assume it has been de-registered. Generally they all have to do with a detected degradation in signal quality which may be caused by a variety of factors. For instance, the peripheral may have gone out-of-range or have been shadowed. Alternatively, the peripheral's battery may have run down or the peripheral was shut-off. Regardless of the cause, de-registration is not a catastrophic event and the peripheral may quickly be re-registered, once the obstruction to signal quality has been resolved, using the process described in section 3.4.3 Re-registering peripherals.

A degradation in signal quality is detected by errors in protocol execution. For example, a failure to acknowledge several consecutive pages or polls is grounds for the access point to the drop the peripheral. Similarly, a peripheral encountering several polling intervals without being polled may assume the access point has de-registered it. Other events warranting de-registration include an abrupt and sustained failure in the isochronous transfer or a failure by the peripheral to decode a substantial number of consecutive BA bursts.

An access point will de-register a peripheral when counters NA203 and NA204 have been exceeded. Also a peripheral will be de-registered when timer TA205 has expired. Finally, a peripheral may de-registered if it has not re-registered as required by the DRX standby mode.

A peripheral will attempt to re-register will a system when timers NP202 and NP203 have been exceeded. Also a peripheral will attempt re-register when timer TP205 has expired. Finally, a peripheral may re-register as required by the DRX standby mode.

The re-registration process happens regularly in the normal course of protocol operation and may be executed in an expedient manor.

FIG. 27, numeral 2700, illustrates the flow-chart for the re-registration process. The flow chart has two entry points,

one for peripherals currently synchronized to the system and the other for peripherals in a unsynchronized state. The process is similar to the normal registration process in that the frequency search (2702) is employed followed by a registration request. However, the re-registration process allows an access point which identifies a familiar peripheral to respond with a registration assignment containing the identical Peripheral ID issued on the initial registration. The peripheral recognizing the familiar Peripheral ID associated with System Specific ID may resume registered operation assuming that all negotiated parameters remain as before. Optionally, a peripheral or access point may forgo the shortened re-registration process. A peripheral choosing to forgo the process would begin the service negotiation phase while access point may forgo the process by assigning a new Peripheral ID in the registration assignment.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative and not restrictive. The scope of the invention is, therefore, indicated by the appended claims rather than by the foregoing description. All changes which come within the meaning and range of equivalency of the claims are to be embraced within their scope.

We claim:

1. A method for providing low complexity dynamic persistence for random access in a wireless communication system, comprising the steps of:

A) registering, by an access point device, a plurality of peripheral devices;

B) determining, by the access point device, a persistence level based on a number of peripherals in the plurality of peripheral devices;

C) setting, by the access point device, a source address within a block assignment to a contention address and the persistence level;

D) broadcasting, by the access point device, the block assignment;

E) identifying, by each peripheral device, the contention address and reading the persistence level;

F) generating, by each peripheral device, a random number based on the persistence level;

G) determining, by each peripheral device, whether the random number is equal to zero;

H) transmitting, by any peripheral device for which the random number is equal to zero, a payload burst containing a resource request;

I) deferring transmission of a payload burst, by any peripheral for which the random number fails to equal zero;

J) receiving a payload burst, by the access point device; and

K) acknowledging, by the access point, reception of the payload burst and which peripheral device transmitted the payload burst.

2. A method for providing low complexity dynamic persistence for random access by a peripheral device in a wireless communication system, comprising the steps of:

A) receiving a block assignment having a source address which contains a contention address and a persistence level;

B) identifying the contention address and reading the persistence level;

C) generating a random number based on the persistence level;

D) determining whether the random number is equal to zero; and

E) transmitting when the random number is equal to zero and deferring transmission when the random number fails to equal zero.

3. A method for providing low complexity dynamic persistence for random access by an access point device in a wireless communication system, comprising the steps of:

A) registering a plurality of peripheral devices;

B) determining a persistence level based on a number of peripheral devices in the plurality of peripheral devices;

C) setting a source address within a block assignment to a contention address and the persistence level;

D) broadcasting the block assignment;

E) determining whether a payload burst has been received; and

F) acknowledging,where a payload burst has been received, reception of the payload burst and which peripheral device transmitted the payload burst.

4. The method of claim 3 where acknowledging includes assigning a number of blocks based on the resource request sent by the peripheral transmitting the payload burst.

5. The method of claim 3 where acknowledging includes assigning a destination address in a next block assignment which contains a source address equal to the contention address.

6. A peripheral device for providing low complexity dynamic persistence for random access in a wireless communication system, comprising:

A) a block assignment receiver, for receiving a block assignment having a source address which contains a contention address and a persistence level and identifying the contention address and reading the persistence level;

B) a random number generator, coupled to the persistence based transmitter , for generating a random number based on the persistence level; and

C) a persistence based transmitter, coupled to the random number generator and to the block assignment receiver, for transmitting a payload burst containing a resource request based on the random number and the persistence level.

7. The peripheral device of claim 6 wherein the random number generator is a linear feedback shift register generating a pseudorandom binary sequence wherein a number of bits generated by the linear feedback shift register is based on the persistence level and the persistence based transmitter transmits the payload burst when the bits generated are all equal to zero.

8. The peripheral device of claim 6 wherein the peripheral device is one of:

A) a wireless speaker;

B) a cordless telephone;

C) a shared printer;

D) a networked game;

E) a peripheral personal computer;

F) a child's toy;

G) a video electrical device;

H) an audio electrical device; and

I) a set top box.

9. An access point device for providing low complexity dynamic persistence for random access in a wireless communication system, comprising:

A) a device manager, arranged to receive registration requests from a plurality of peripheral devices, for registering the plurality of peripheral devices and determining a persistence level based on a number of peripheral devices in the plurality of peripheral devices;

B) an efficient persistence scheduler, coupled to the device manager and a receiver, for setting a source address within a block assignment to a contention address and the persistence level;

C) a transmitter, coupled to the efficient persistence scheduler, for broadcasting the block assignment; and

E) the receiver, coupled to the efficient persistence scheduler and arranged to receive a payload burst, for determining whether the payload burst containing a resource request has been received and where a payload burst has been received, passing the resource request to the scheduler, which acknowledges reception of the resource request and which peripheral device transmitted the payload burst in a subsequent block assignment.

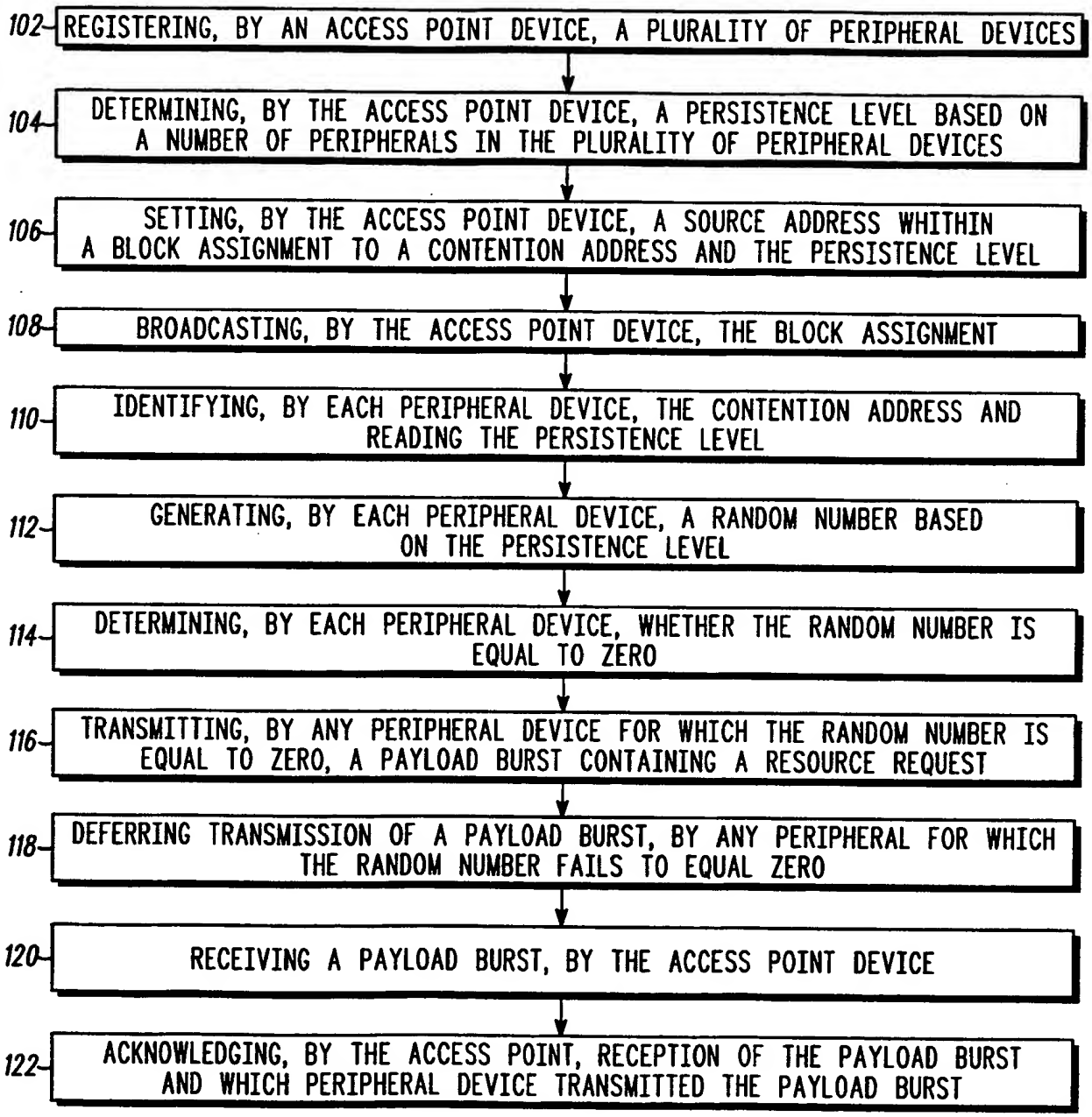


FIG.1 100

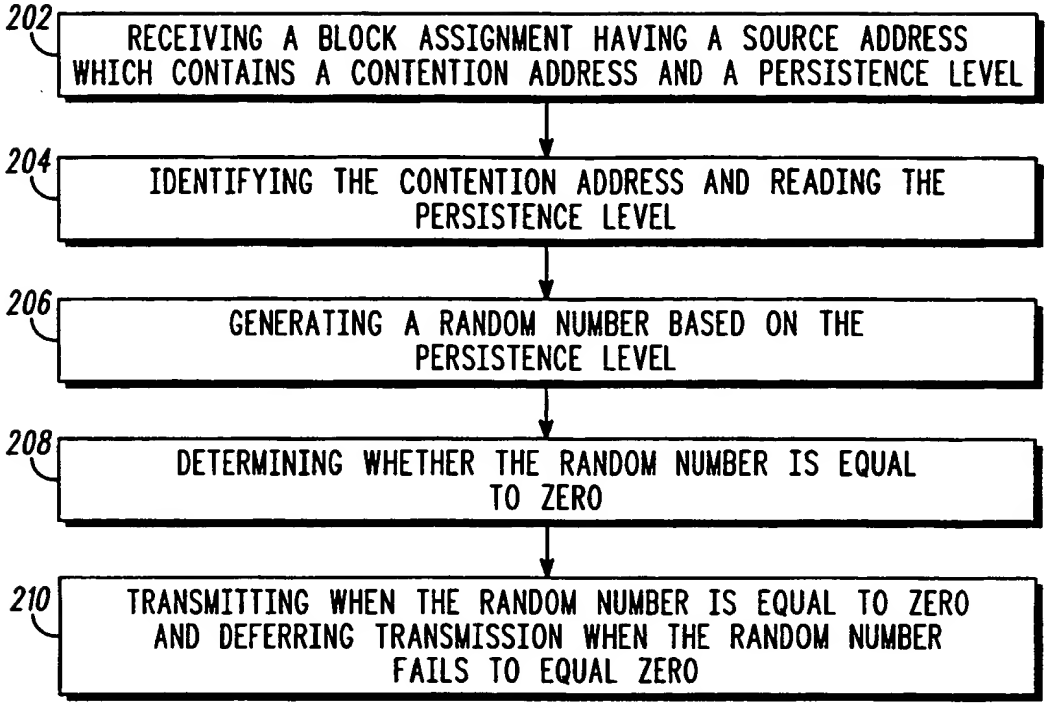


FIG.2 200

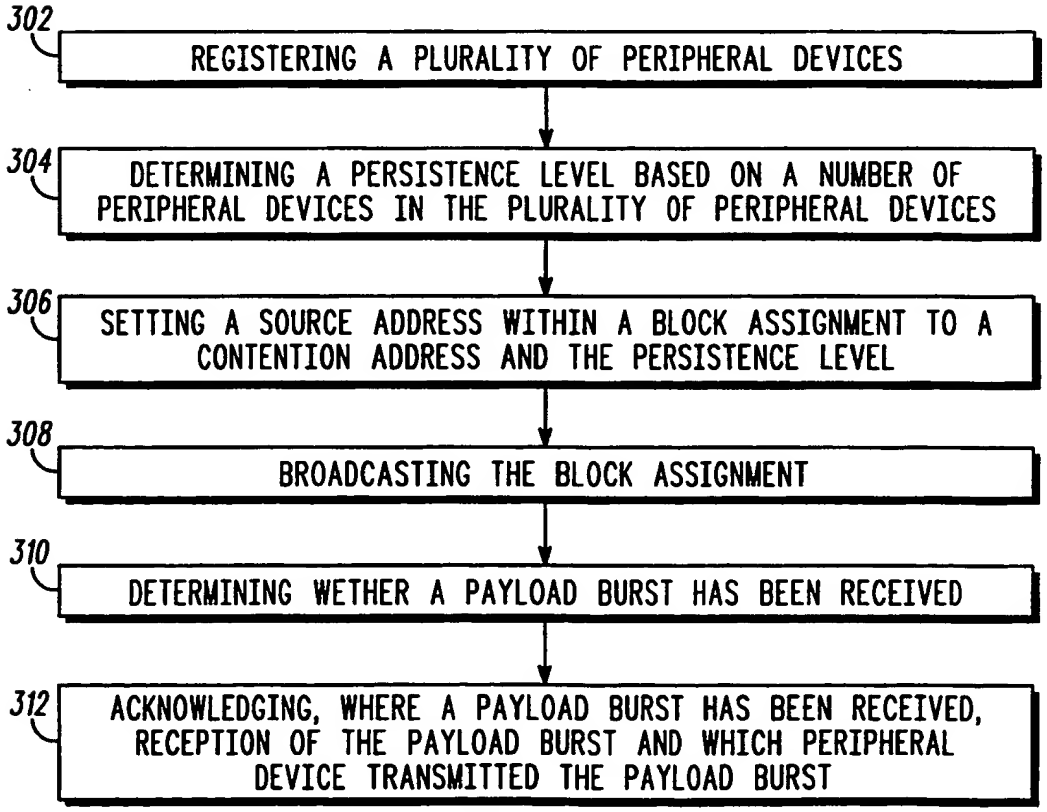


FIG.3 300

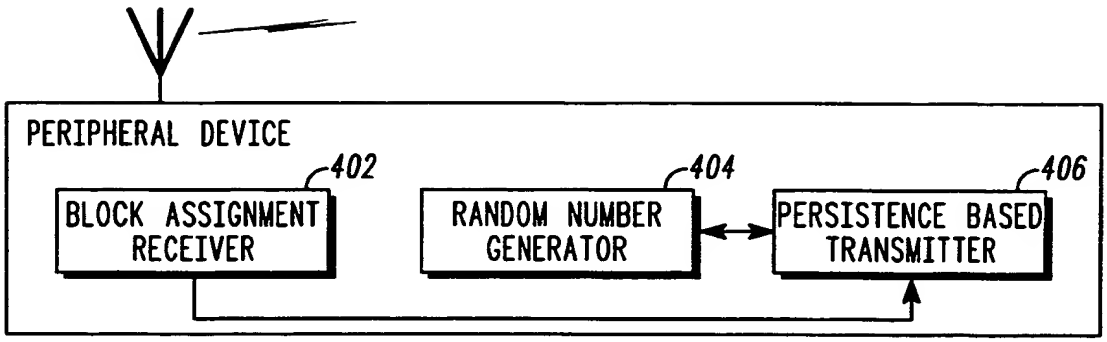


FIG.4 400

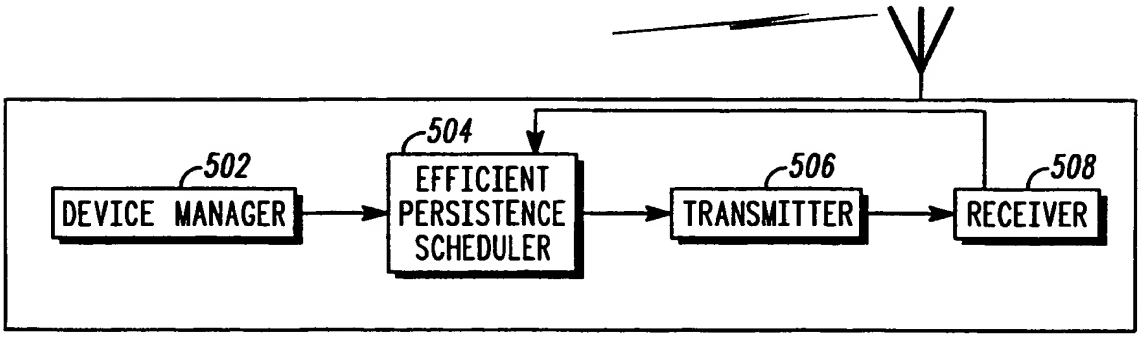


FIG.5 500

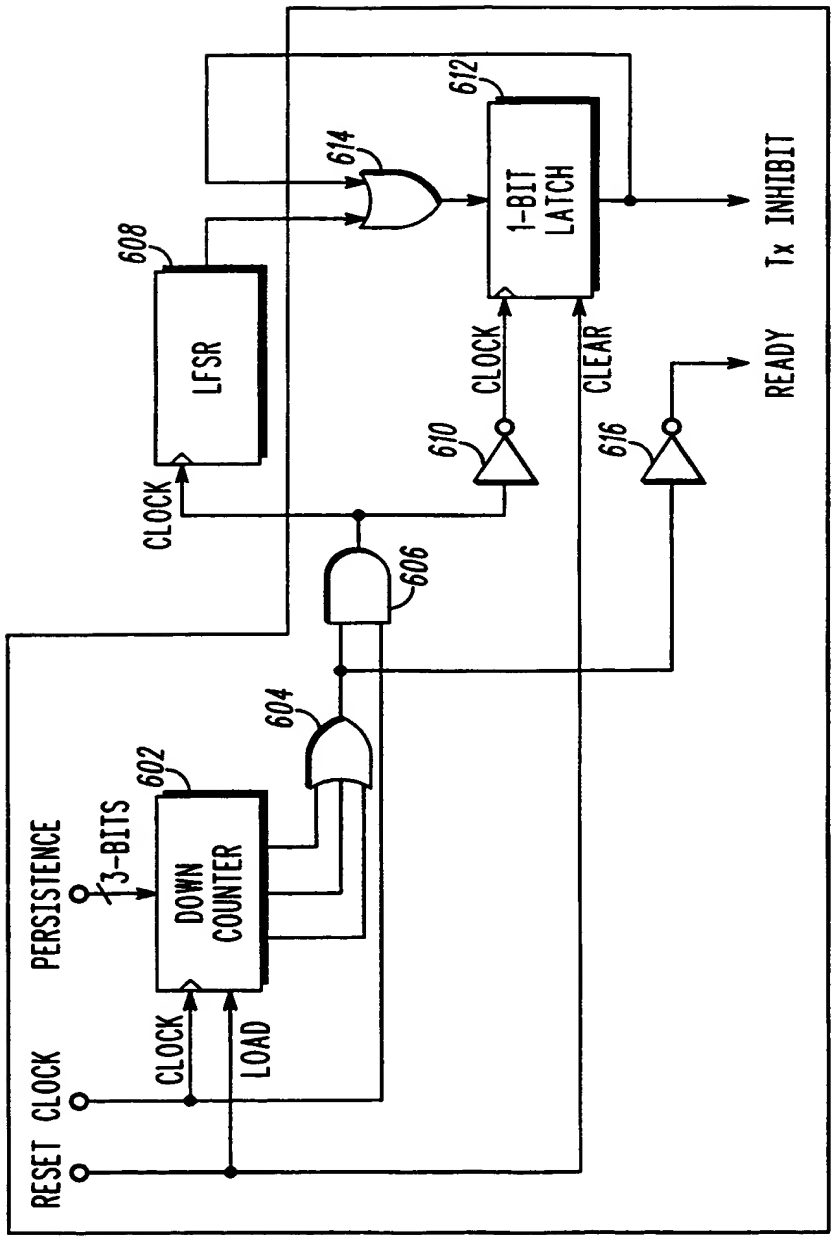


FIG.6

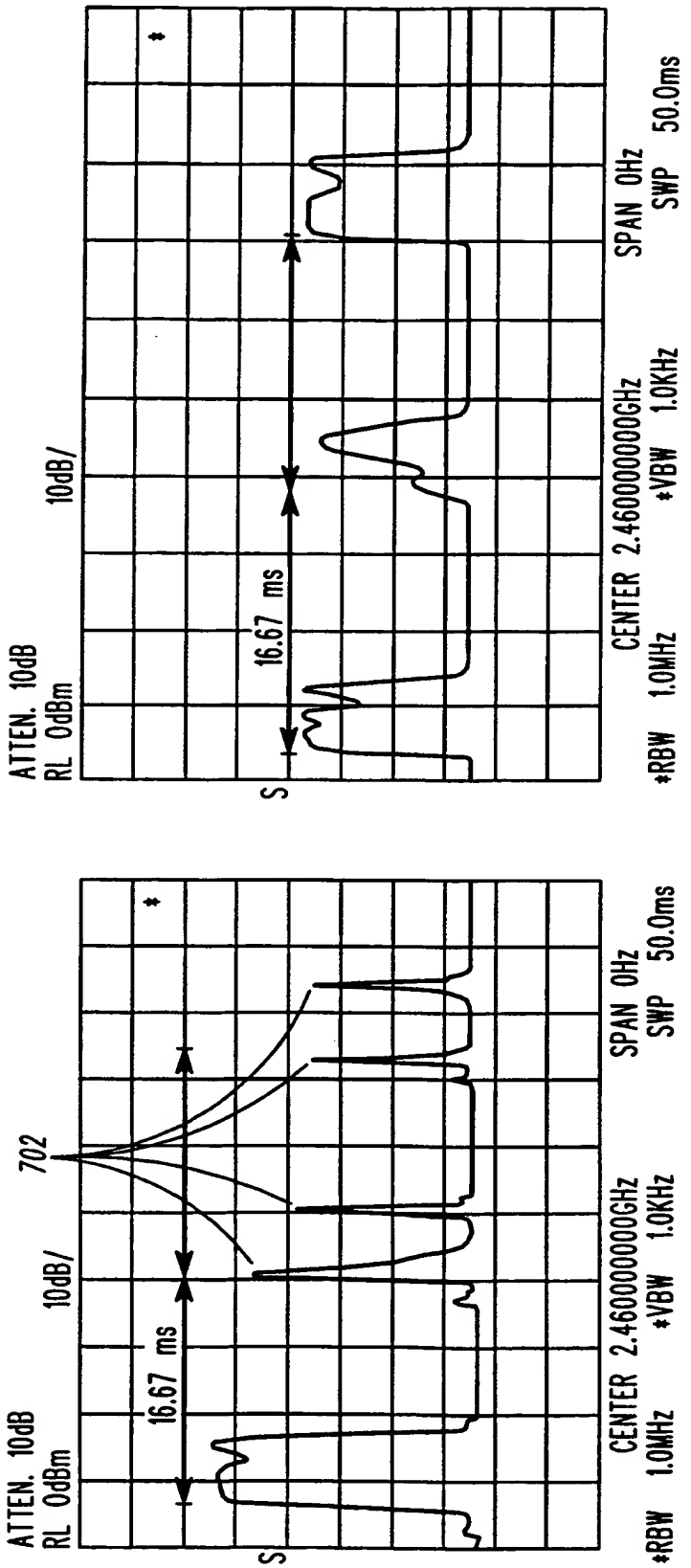


FIG.7 700

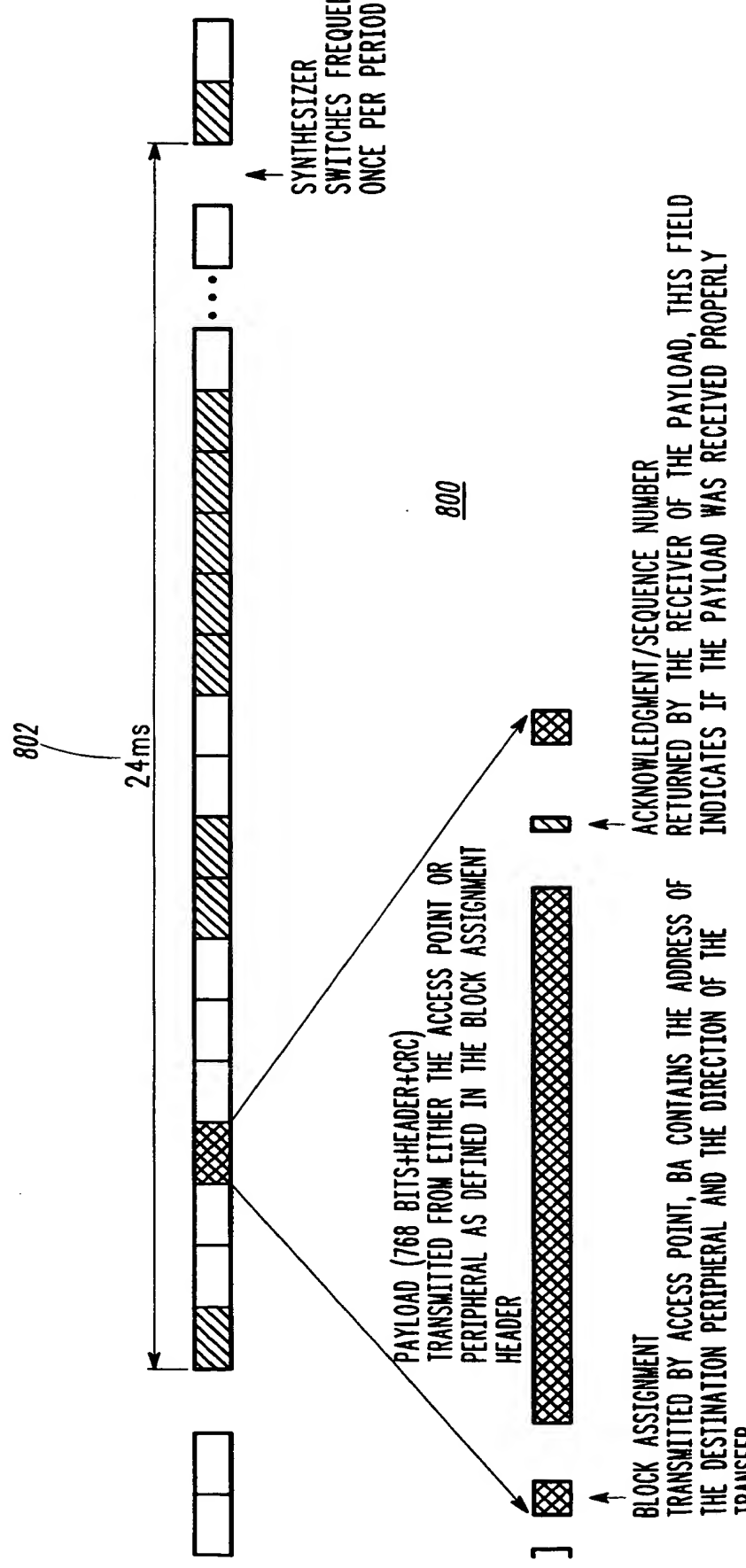


FIG.8

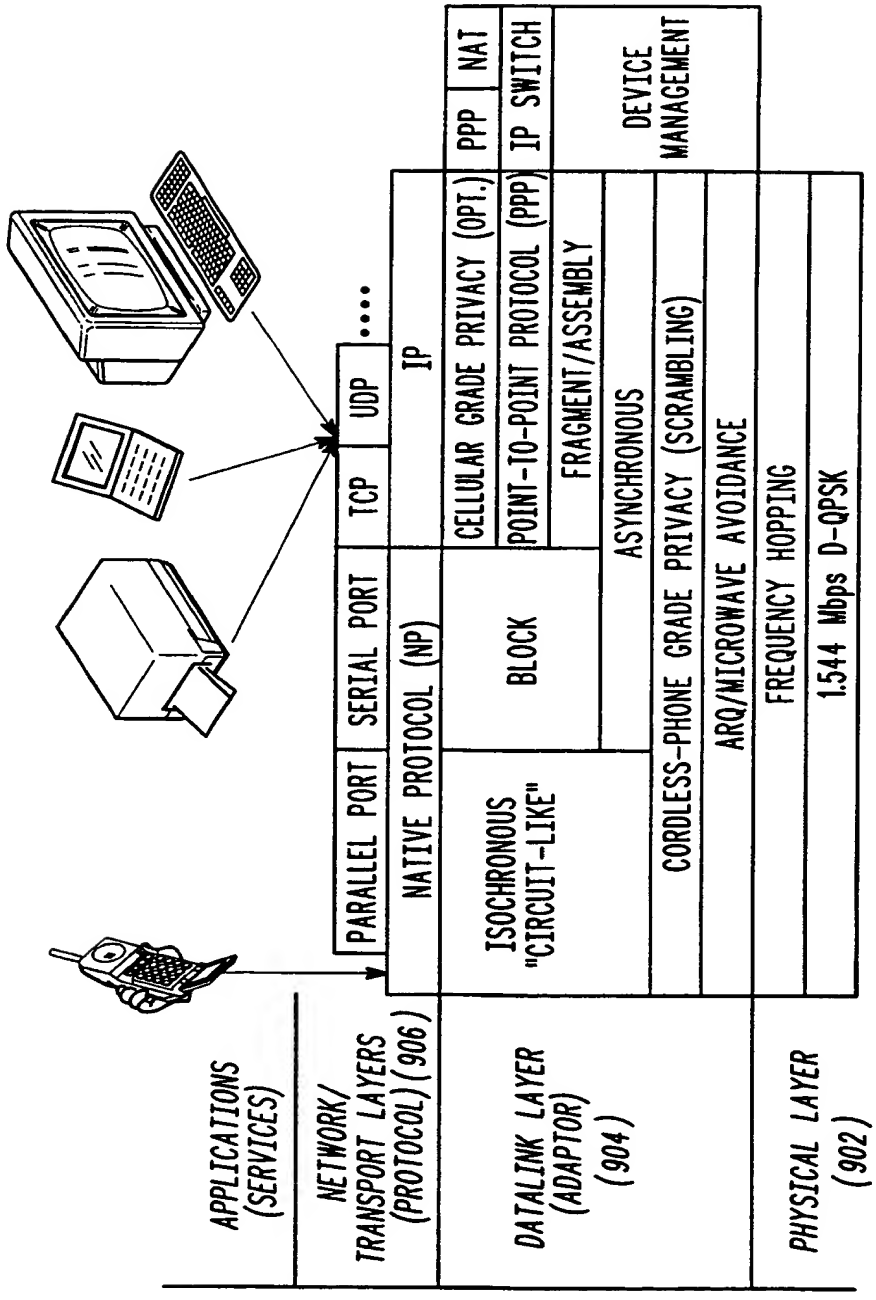


FIG.9 900

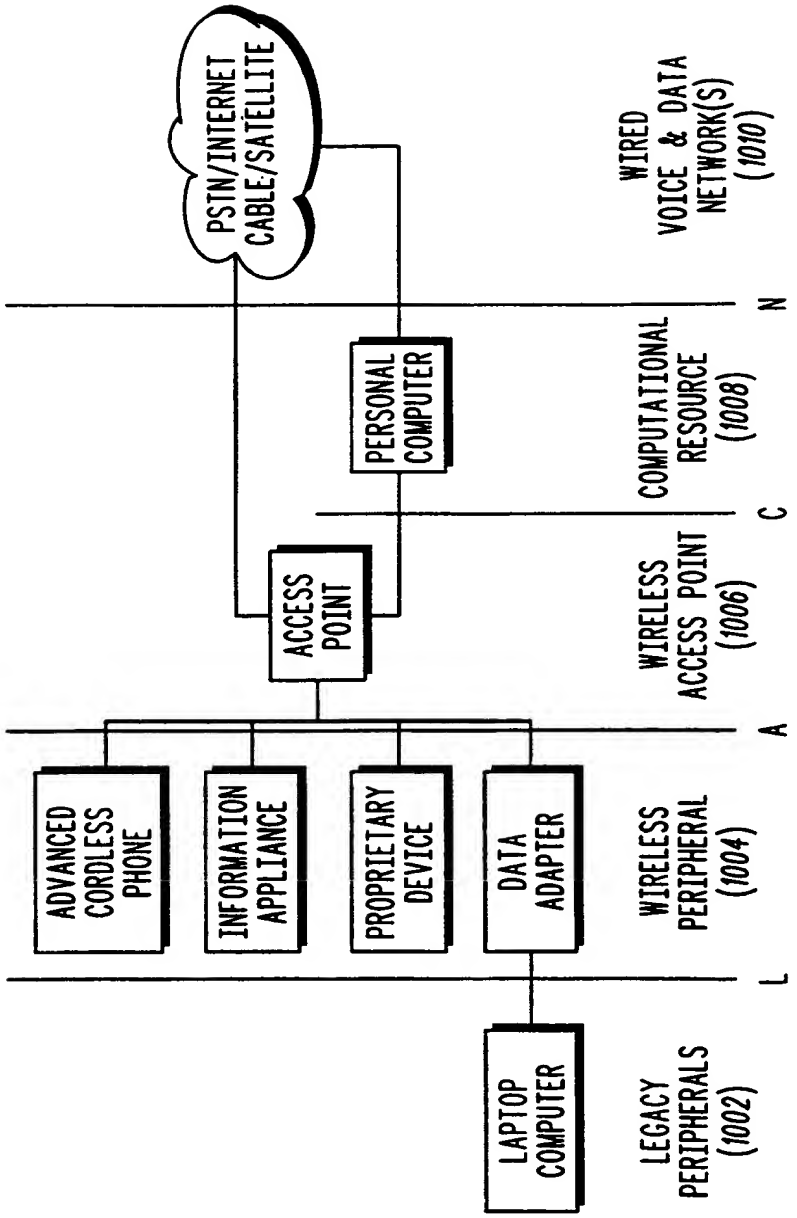


FIG.10 1000

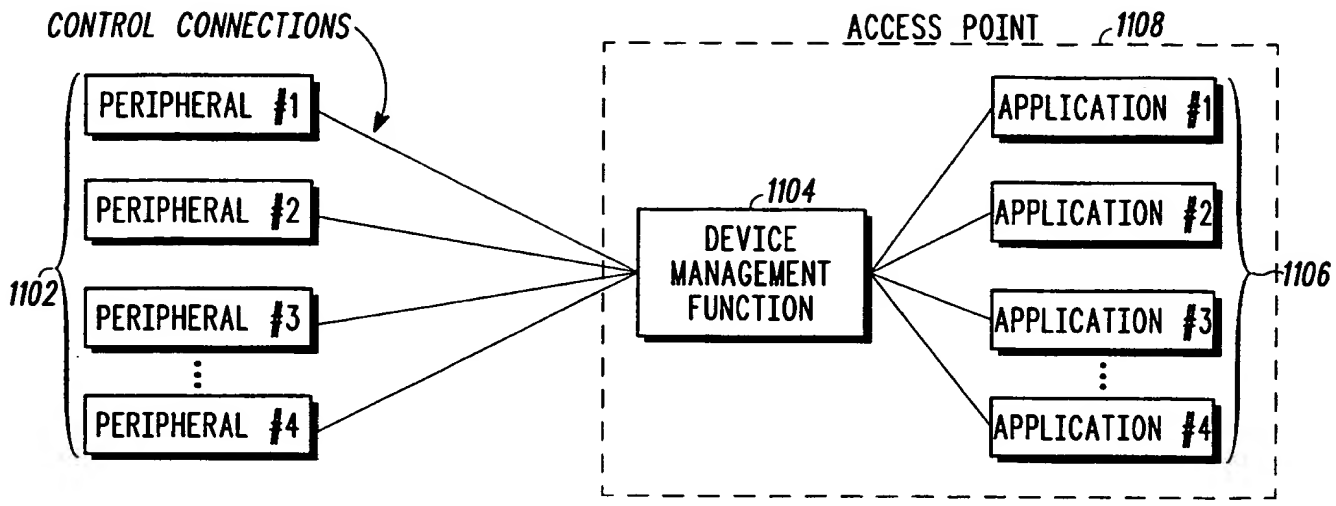


FIG.11 1100

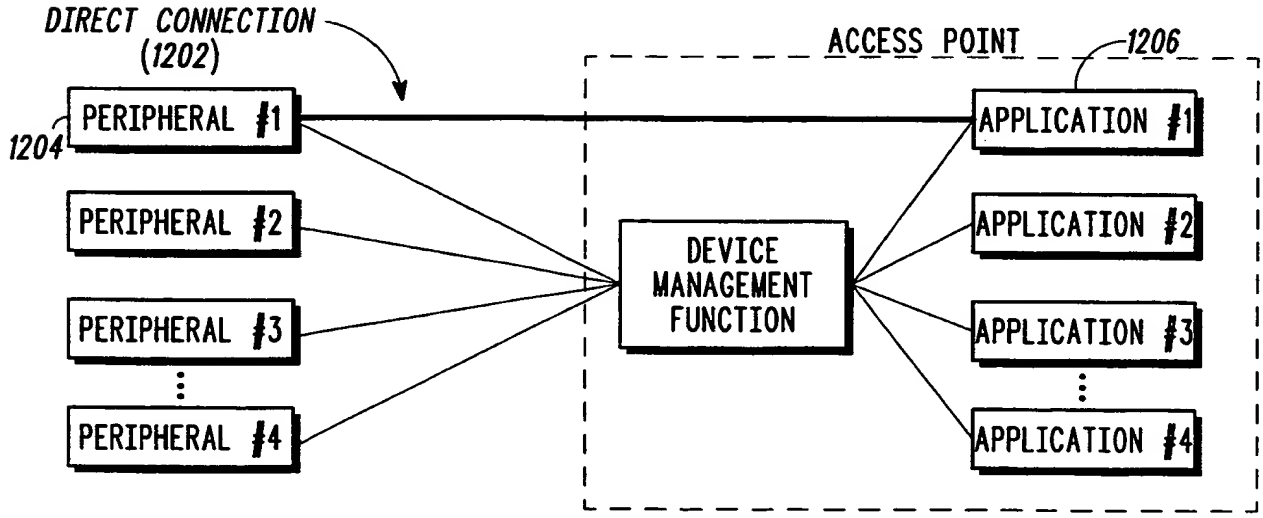


FIG.12 1200

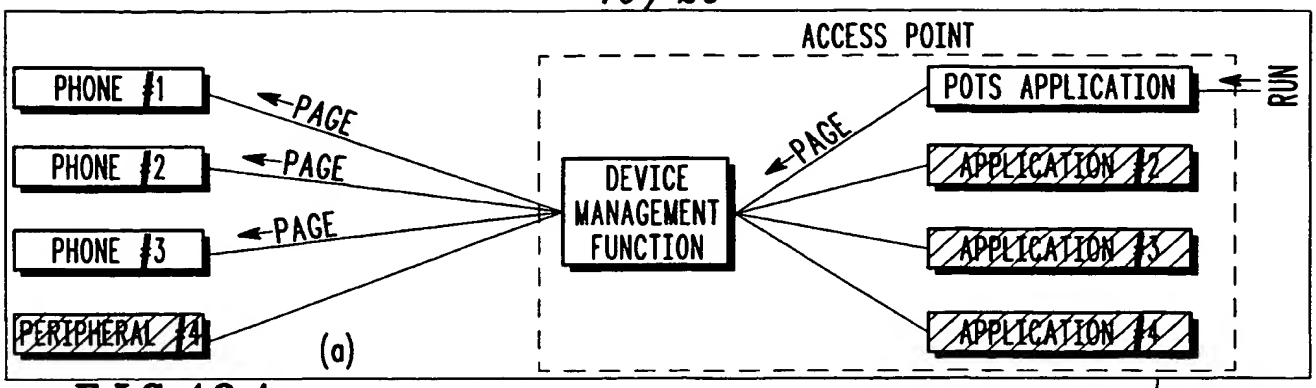


FIG.13A

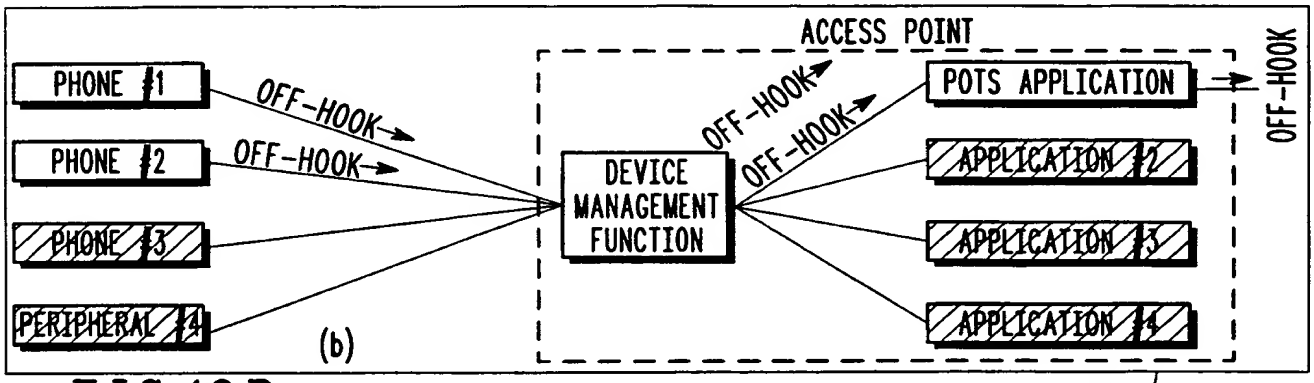


FIG.13B

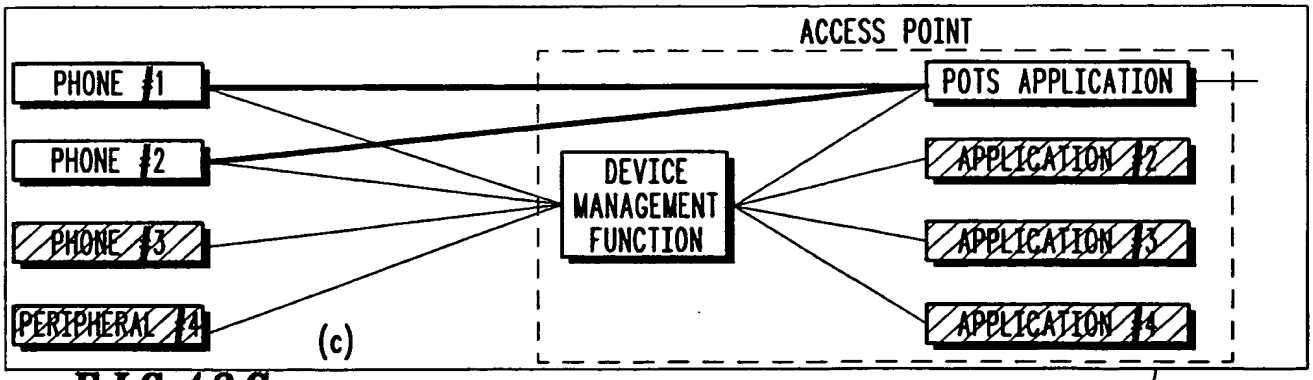


FIG.13C

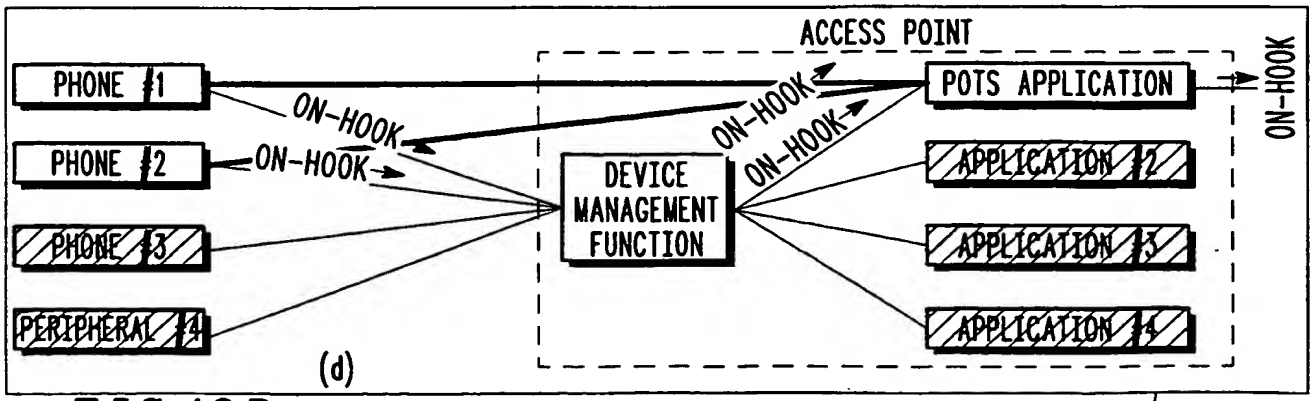


FIG.13D

1300

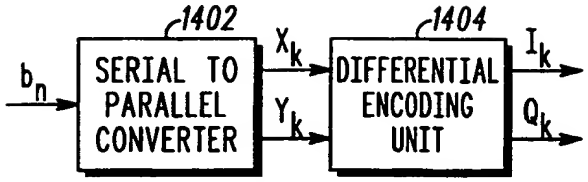


FIG.14 1400

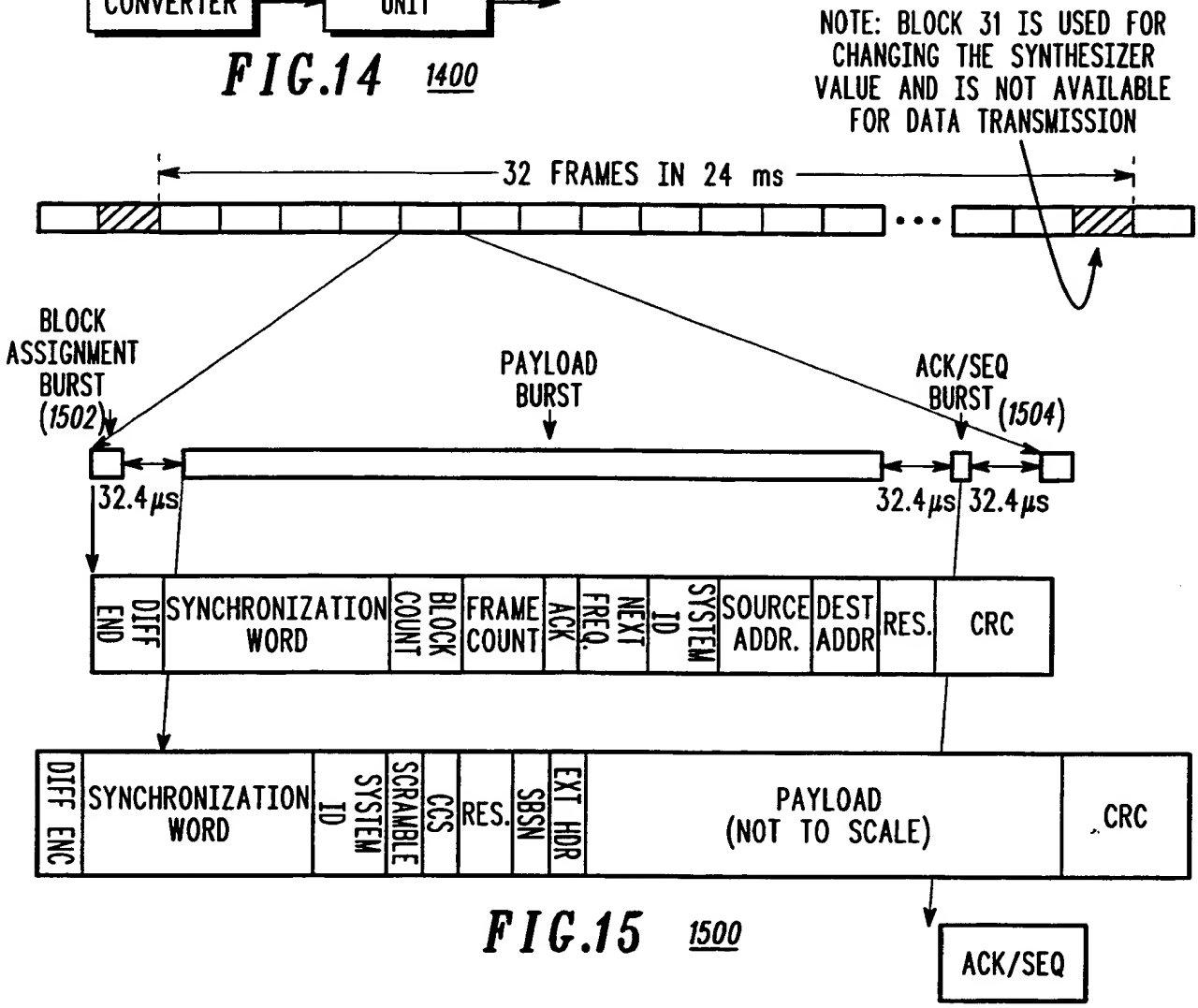


FIG.15 1500

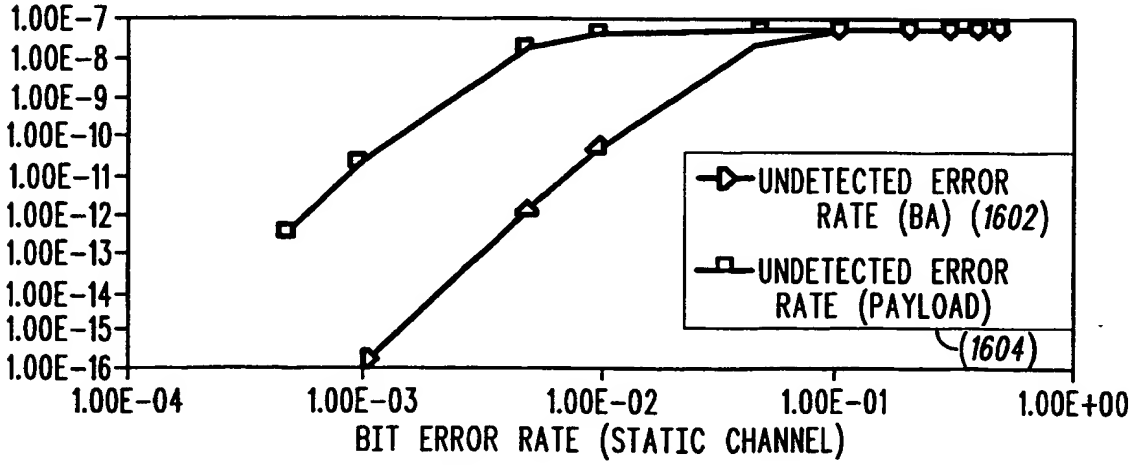


FIG.16 1600

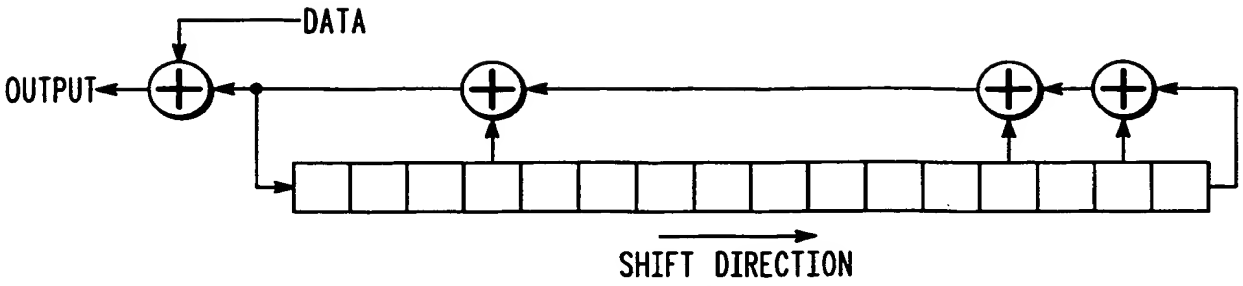


FIG.17

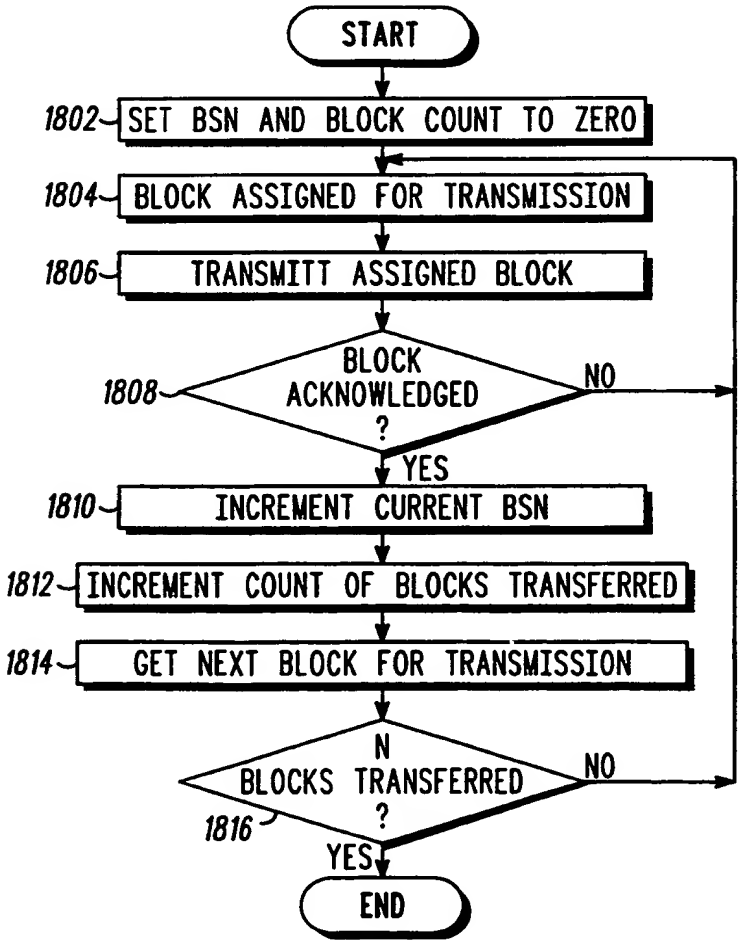


FIG.18 1800

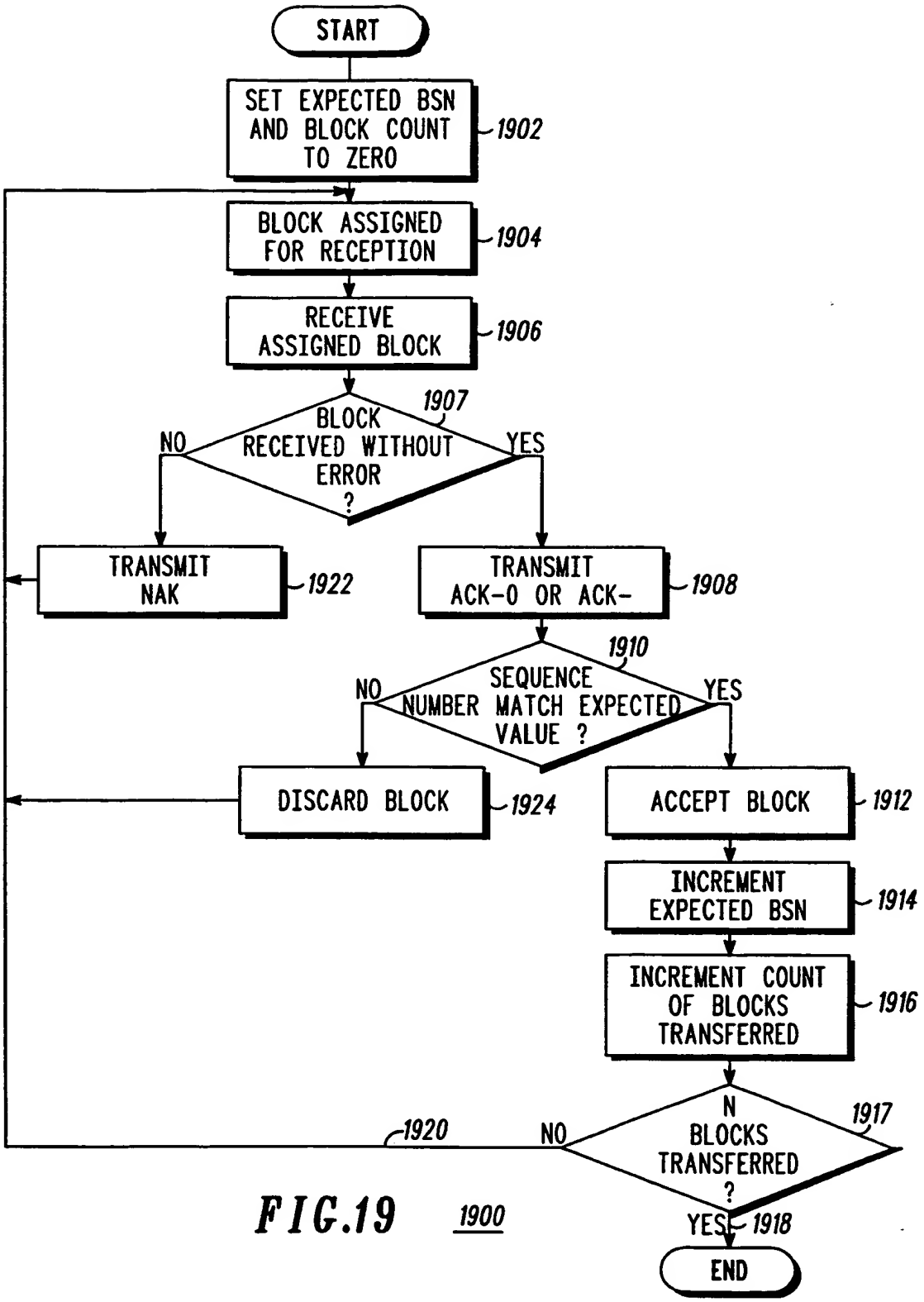


FIG.19 1900

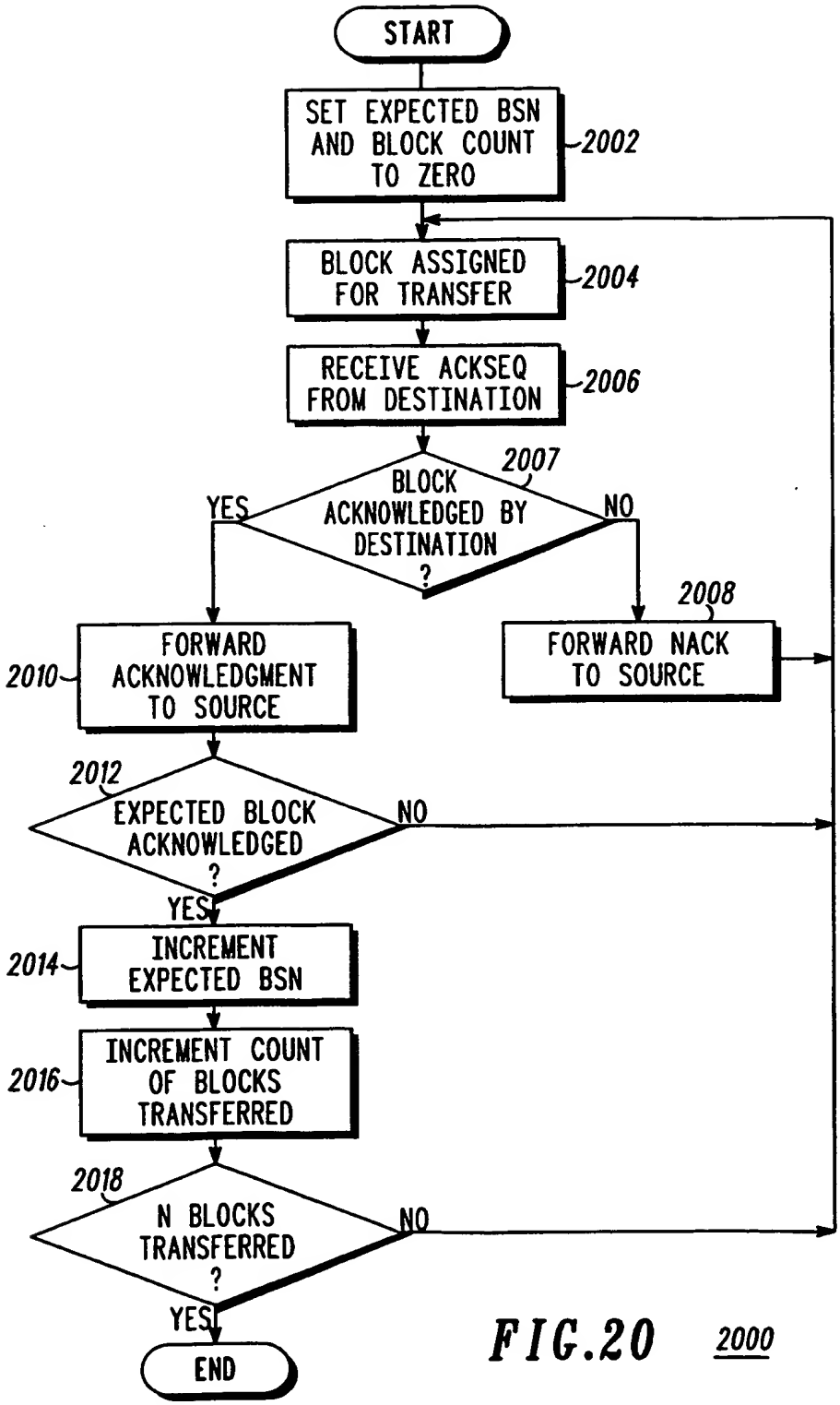


FIG.20 2000

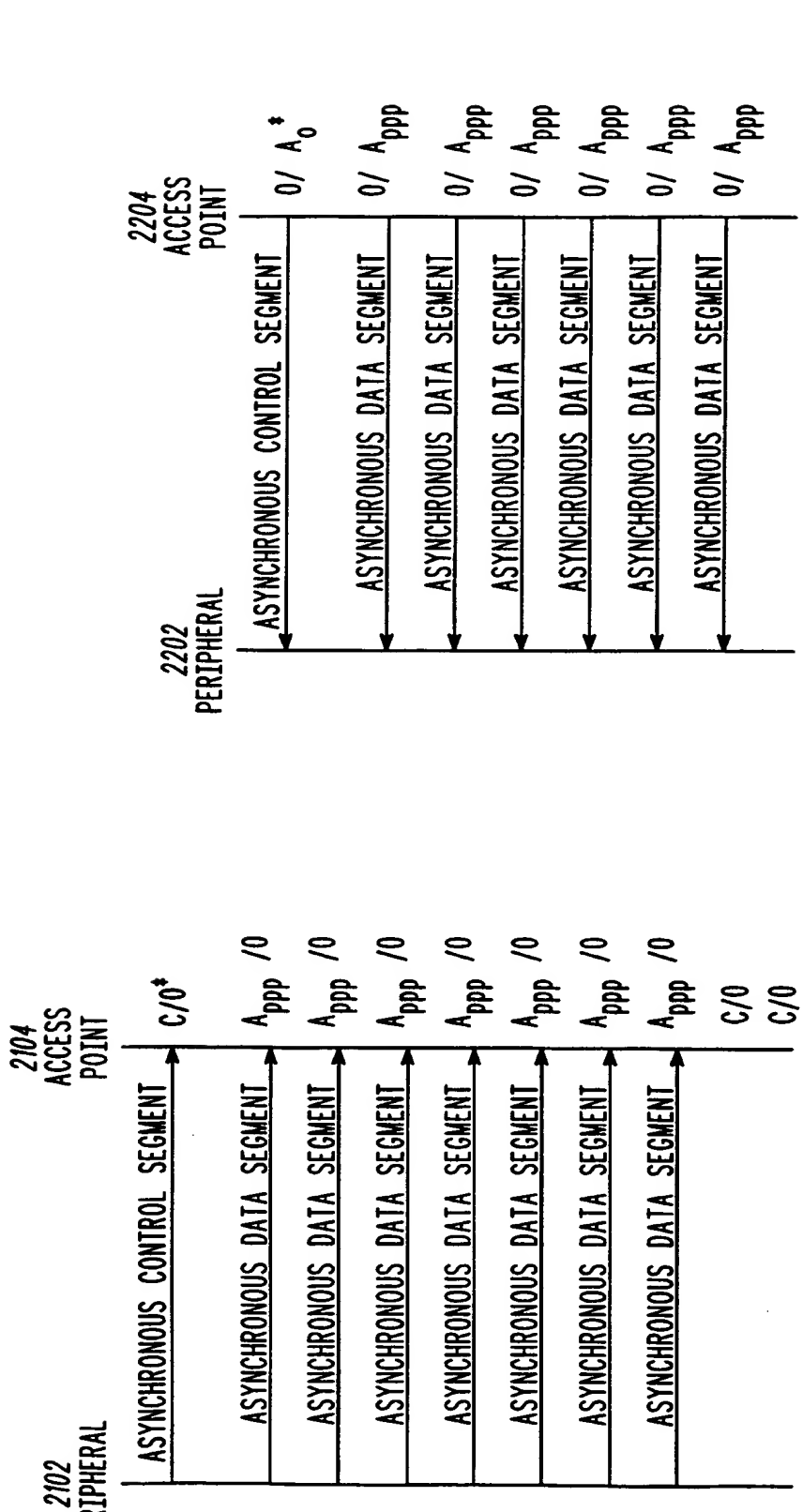
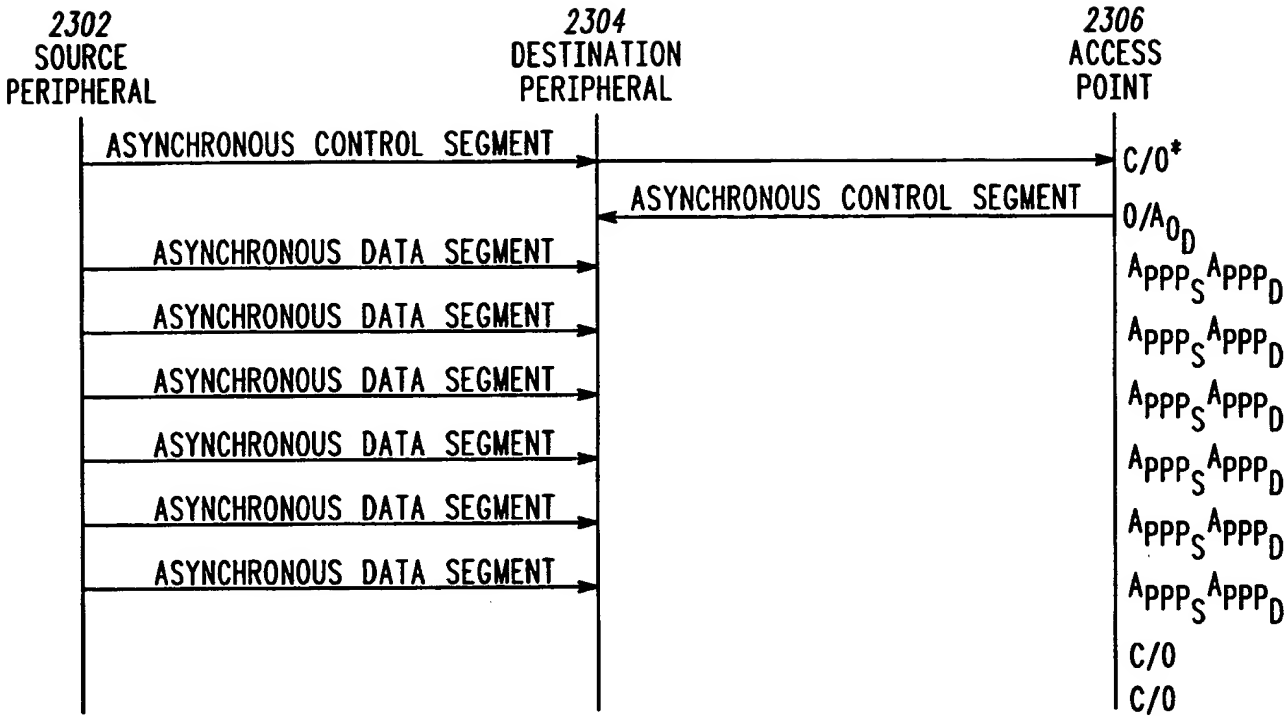


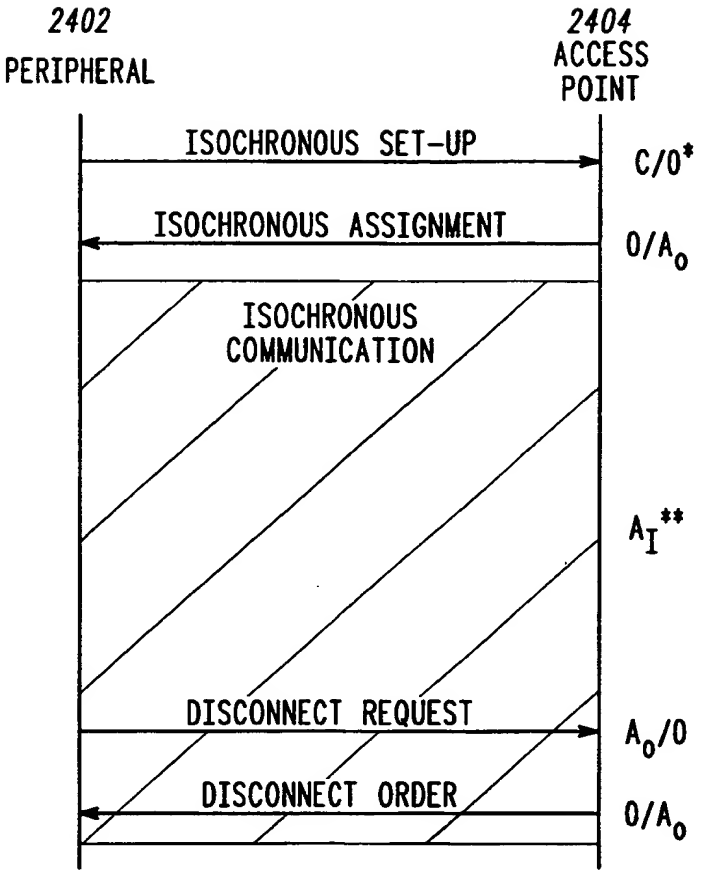
FIG.21 2100

FIG.22 2200



*DENOTES THE BLOCKS SOURCE/DESTINATION ADDRESS.
"O" SIGNIFIES THE NULL ADDRESS

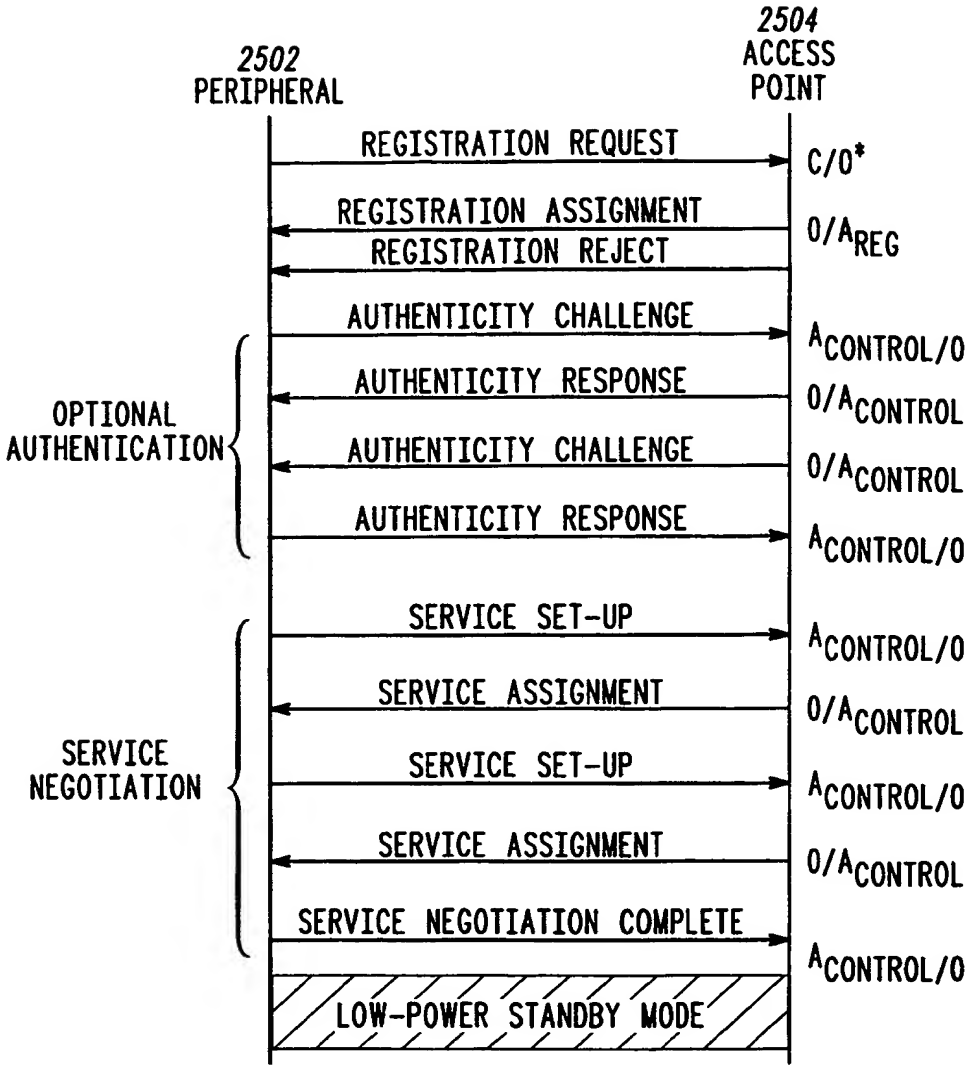
FIG.23 2300



* DENOTES THE BLOCKS SOURCE/DESTINATION ADDRESS. "0" SIGNIFIES THE NULL ADDRESS

** A SPECIAL SUB-ADDRESS IS ASSIGNED TO EACH ISCHRONOUS CONNECTION

FIG.24 2400



* DENOTES THE BLOCKS SOURCE/DESTINATION ADDRESS.
"O" SIGNIFIES THE NULL ADDRESS

FIG.25 2500

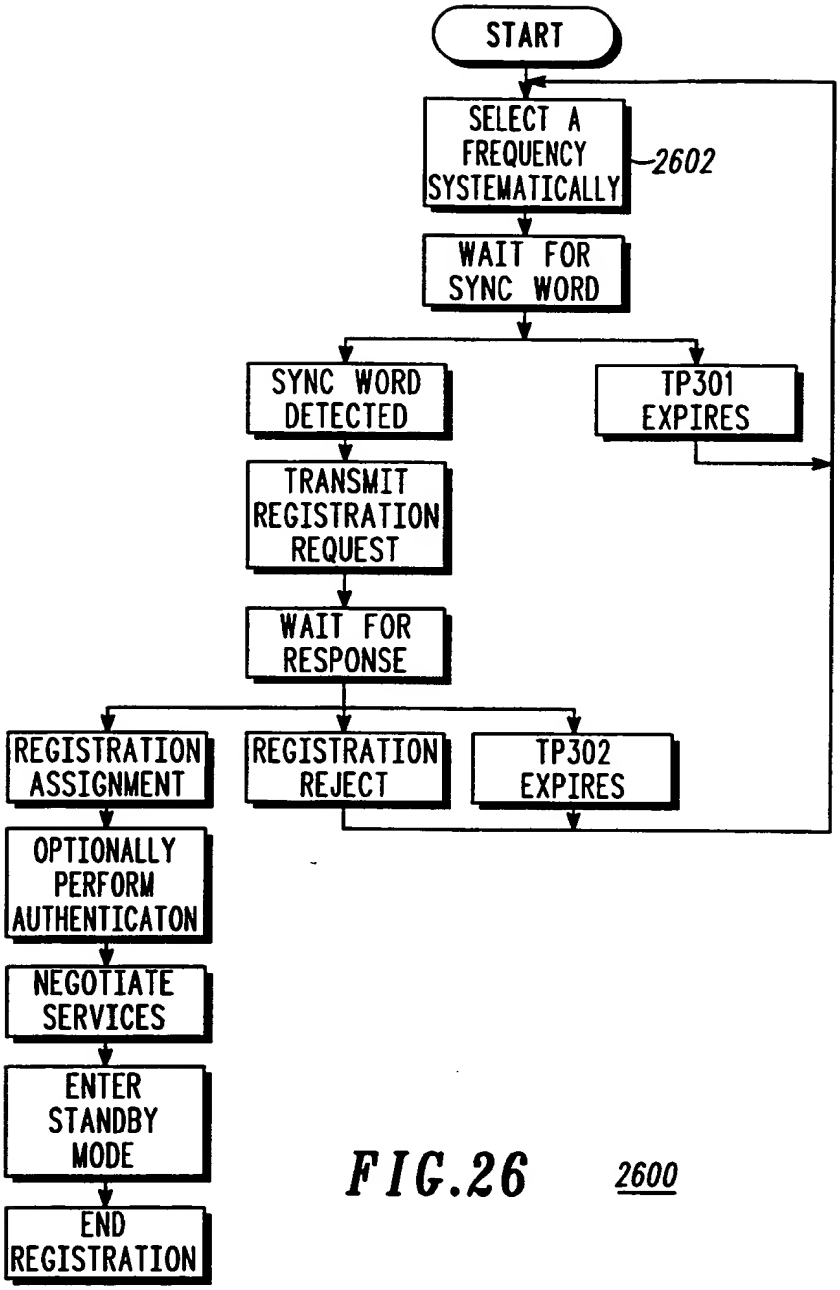


FIG.26 2600

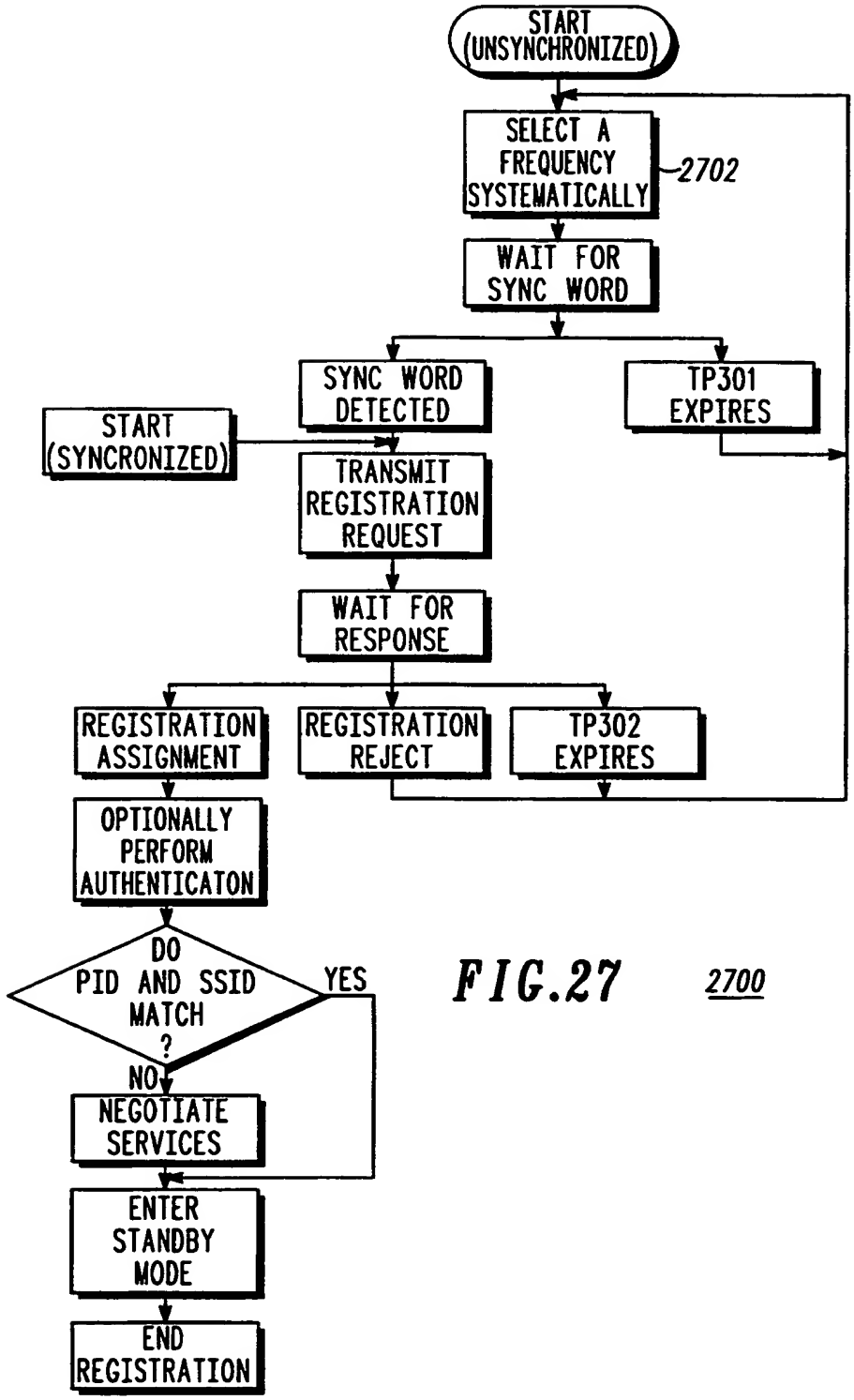


FIG.27 2700

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/14070

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04H 1/00
US CL :455/6.3

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 455/6.3, 3.1, 352, 353; 348/8, 734; 341/176; 379/102.02, 102.03

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,471,668 A (SOENEN et al) 28 November 1995, col. 2, lines 1-6.	1-3, 6 and 9
A	US 4,665,544 A (HONDA et al) 12 May 1987, col. 1, line 61 - col. 2, line 68.	1-3, 6 and 9
A	US 5,666,363 A (OSAKABE et al) 09 September 1997, col.. 4, line 32 - col. 6, line 16.	1-3, 6 and 9
A	US 4,989,081 A (MIYAGAWA et al) 29 January 1991, col. 1, line 39 - col. 2, line 36.	1-3, 6 and 9
A	US 4,935,924 A (BAXTER) 19 June 1990, col. 1, line 41 - col. 2, line 47.	1-3, 6 and 9

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 SEPTEMBER 1998	Date of mailing of the international search report 19 OCT 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer VICTOR R. KOSTAK Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet)(July 1992)*